

# Health Insurance Portability and Accountability Act (HIPAA) Policy

## *HIPAA Steering Committee/ Administration*

*SUBJECT: HIPAA Policies and Procedures for Columbus Public Health (CPH)*

*SCOPE: Columbus Public Health, All Staff*

**TOTAL NUMBER OF PAGES:** 67

**REVIEW FREQUENCY:** Every 5 years

**ORIGINAL DATE ADOPTED:** 6/1/1992

**LATEST EFFECTIVE DATE:** 1/4/2013

**REVIEW/REVISION DATE(S):** 6/1/1992, 1/22/2003, 3/4/2003, 3/11/2003, 3/4/2003, 3/21/2003, 7/2/2003, 8/4/2003, 11/18/03, 4/20/04, 3/17/2005, 12/27/2010, 01/15/2011, 11/5/2012, 1/4/13

**PRIMARY AUTHOR(S):** Shelly Mitchell, RHIA, Health Information Manager  
Sandra Taylor, RHIA, Franklin County Registrar

**FINAL**

---

**BOARD OF HEALTH APPROVAL DATE:** 12/18/2012

**REFERENCE NUMBER:** See Individual Sections



THE CITY OF  
**COLUMBUS**  
MICHAEL B. COLEMAN, MAYOR

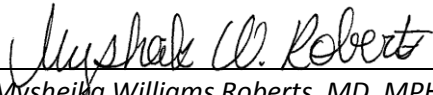
COLUMBUS  
PUBLIC HEALTH

**SIGNATURE PAGE:**

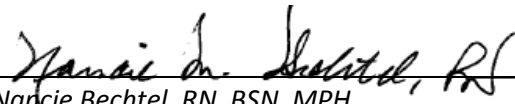
I have reviewed this document and endorse it as an official CPH Policy and Procedure:

  
\_\_\_\_\_  
Teresa Long, MD, MPH  
Health Commissioner

4 / 27 / 2013  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Mysheika Williams Roberts, MD, MPH  
Assistant Health Commissioner/Medical Director


4 / 12 / 13  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Nancie Bechtel, RN, BSN, MPH  
Assistant Health Commissioner/Chief Nursing Officer

3 / 29 / 2013  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Roger Cloern  
Assistant Health Commissioner/Chief Operations Officer

3 / 26 / 13  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Mary Ellen Wewers, PhD, MPH  
Board of Health President

5 / 29 / 13  
\_\_\_\_\_  
Date

## TABLE OF CONTENTS:

<b>HIPAA POLICY .....</b>	<b>4</b>
<b>101-RM INITIATION AND MAINTENANCE OF CLIENT HEALTH RECORDS .....</b>	<b>9</b>
<b>102-RM SAFEGUARDING PROTECTED HEALTH INFORMATION .....</b>	<b>11</b>
<b>201.1-RM CONFIDENTIALITY POLICY .....</b>	<b>13</b>
<b>202.1-RM AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION (PHI).....</b>	<b>14</b>
<b>202.2-RM ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION .....</b>	<b>16</b>
<b>202.3-RM MINIMUM NECESSARY USE OF PROTECTED HEALTH INFORMATION .....</b>	<b>18</b>
<b>202.4-RM NOTICE OF PRIVACY PRACTICE .....</b>	<b>19</b>
<b>203-RM DISCLOSURE OF CLIENT INFORMATION- HIV TESTING OR TREATMENT.....</b>	<b>20</b>
<b>204-RM DISCLOSURE OF CLIENT INFORMATION- DRUG AND ALCOHOL ABUSE PROGRAMS.....</b>	<b>22</b>
<b>209-RM RESPONDING TO A SUBPOENA OR COURT ORDER.....</b>	<b>25</b>
<b>210-RM CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION VIA FACSIMILE (FAX) AND ELECTRONIC MAIL (EMAIL) .....</b>	<b>30</b>
<b>211-RM BUSINESS ASSOCIATE PRIVACY AGREEMENTS .....</b>	<b>32</b>
<b>212-RM HIPAA CLIENT COMPLAINT PROCESS.....</b>	<b>33</b>
<b>213-RM RELEASE OF PROTECTED HEALTH INFORMATION OF CLIENTS EXPERIENCING ABUSE, NEGLECT AND/OR DOMESTIC VIOLENCE .....</b>	<b>35</b>
<b>214-RM PERSONAL REPRESENTATIVES' ROLE IN THE RELEASE OF PROTECTED HEALTH INFORMATION .....</b>	<b>38</b>
<b>215-RM DISCLOSURE OF PROTECTED HEALTH INFORMATION RELATED TO ORGAN AND TISSUE DONATIONS .....</b>	<b>39</b>
<b>216-RM CONSENT TO PHOTOGRAPH CLIENTS AND/OR USE OF CLIENTS' STATEMENTS.....</b>	<b>39</b>
<b>217-RM VERIFICATION OF CALLERS ON TELEPHONE REQUESTS FOR PROTECTED HEALTH INFORMATION .....</b>	<b>40</b>
<b>218-RM DISCLOSURE OF PSYCHOTHERAPY NOTES .....</b>	<b>41</b>
<b>219-RM APPROPRIATE AUTHENTICATION AND SIGNATURES FOR CONSENT TO RELEASE PROTECTED HEALTH INFORMATION.....</b>	<b>42</b>
<b>220-RM PROCESSING WRITTEN REQUESTS FOR PROTECTED HEALTH INFORMATION .....</b>	<b>44</b>
<b>221-RM DISCLOSURE OF PROTECTED HEALTH INFORMATION TO HEALTH SYSTEM OVERSIGHT ENTITIES AND OTHER GOVERNMENTAL ENTITIES .....</b>	<b>46</b>
<b>222-RM DISCLOSURE OF CLIENT INFORMATION - MASS VACCINATIONS .....</b>	<b>48</b>
<b>223-RM RELEASE OF PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT .....</b>	<b>50</b>
<b>225-RM PUBLIC HEALTH PHI DISCLOSURES .....</b>	<b>53</b>
<b>226-RM RELEASE OF PUBLIC HEALTH INFORMATION TO THE MEDIA.....</b>	<b>56</b>
<b>304-RM SECURITY OF PROTECTED HEALTH INFORMATION STORED ELECTRONICALLY .....</b>	<b>58</b>
<b>306-RM HIPAA QUALITY ASSURANCE MONITOR .....</b>	<b>61</b>
<b>307-RM NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION .....</b>	<b>63</b>
<b>HIPAA FORMS.....</b>	<b>66</b>
<b>INDEX.....</b>	<b>68</b>

# HIPAA Policy

## PURPOSE

- The intent of this document is to instruct all Columbus Public Health programs and employees regarding the use and disclosure of protected health information (PHI), necessary authorization for such use or disclosure and , when use/disclosure is for uses outside of those permitted or required by law.

## POLICY

All Columbus Public Health (CPH) programs and divisions shall adhere to the standards as described in this document.

## BACKGROUND

N/A

## GLOSSARY OF TERMS

The following are relevant to this document:

### I. Who is Covered by HIPAA?

- A. **Health care clearinghouses** – A public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements
- B. **Health care provider such as CHD** – A provider of medical or other services, and any other person furnishing health care services or supplies; any person or organization that furnishes, bills, or is paid for healthcare in the normal course of business.
- C. **Health plan** – An individual or group plan that provides or pays the cost of medical care.

### II. Other Key HIPAA Terms:

- A. **Access**: The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
- B. **Authorization** – A signed form containing prescribed elements required for specific and nonroutine uses of protected health information (PHI).
- C. **Breach**: The acquisition, access, use, or disclosure of PHI in a manner that compromises the security or privacy of the PHI to the point of posing a significant risk in financial, reputational, or other harm to the individual.

NOTE: If the following data elements are **excluded** when releasing PHI, **no breach of PHI has occurred**:

- a) Dates of birth;
- b) Names;
- c) Postal address information, other than town or city, state, and zip code;
- d) Telephone numbers;
- e) Fax numbers;
- f) Electronic mail addresses;
- g) Social security numbers;
- h) Medical record numbers;
- i) Health plan beneficiary numbers;

- j) Account numbers;
  - k) Certificate / license numbers;
  - l) Vehicle identifiers and serial numbers, including license plate numbers;
  - m) Device identifiers and serial numbers;
  - n) Web Universal Resource Locators (URLs);
  - o) Internet Protocol (IP) address numbers;
  - p) Biometric identifiers, including finger and voice prints; and
  - q) Full face photographic images and any comparable images.
- D. **Business Associate (BA)** – A person or organization that performs a function or activity on behalf of a covered entity, but is **not** part of the covered entity, and should therefore be required to accept the same obligations for protecting any individually identifiable health care information that they receive from a covered entity. Examples include attorneys, auditors, accountants, computer vendors, consultants, 3<sup>rd</sup> party administrators, health care clearinghouses, data processing firms, billing firms & other covered entities.
- E. **Business Partner (BP)** – A term used in HIPAA Privacy to identify organizations that perform business functions for a covered entity, and should therefore be required to accept the same obligations for protecting any individually identifiable health care information that they receive from the covered entity.
- F. **Client Health Records** – A client health record, which is a complete, timely and accurate account of events; it must exist to provide evidence of services provided to fulfill purposes such as communication, continuity of care, research and education.
- G. **Code Set** – Under HIPAA, this is any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions. Examples include ICD-9-CM, ICD-10-CM, CPT-4, HCPCS, CDT-2, NDC.
- H. **Consent** – A signed form containing prescribed elements required for all routine uses including treatment, payments, and healthcare operations (QA activities, medical review, legal services, auditing functions, business planning & development, business management & general administrative activities).
- I. **Covered Entity (CE)** – Under HIPAA, this includes any business entity that must comply with HIPAA regulations because of their transmission of protected health information in electronic form. This includes health care providers, health plans and health care clearinghouses. For purposes of HIPAA, health care providers include hospitals, physicians and other caregivers.
- J. **Designated Record Sets** – A group of records maintained by or for a covered entity that includes:
- a. The medical records and billing records about individuals maintained by or for a covered health care provider;
  - b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - c. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For purposes of this rule the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

- K. **Disclosure** – The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
- L. **Electronic Data Interchange (EDI)** – X12 and similar variable length formats for the electronic exchange of structured data. It is sometimes used more broadly to mean any electronic exchange of formatted data.
- M. **Episode** – The various health care services and encounters rendered in connection with identified injury or period of illness.
- N. **Health care** – Prevention, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that which affects the structure or function of the body; or sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
- O. **Health Care Operations** – Include functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals; conduction of or arranging for medical review, legal services, and auditing functions; business planning and development; and general business and administrative activities.
- P. **Health Information** – Any information, whether oral or recorded in any form or medium, that:
1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  2. Relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual.”
- Q. **HIPAA** – Health Insurance Portability and Accountability Act of 1996, which includes electronic standards to improve the efficiency and effectiveness of health care. It also provides protections for the security and privacy of individually identifiable health information.
- R. **Identifiers**: Information about an individual, either taken alone or in combination, which may be used to identify the individual. This includes but is not limited to:
- A. Names;
  - B. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code or geocode, except for the first 3 digits of a zip code, if the Bureau of the Census states that the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and
  - C. the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
  - D. All elements of dates, except the year, for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates, including the year, indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
  - E. Telephone numbers;
  - F. Fax numbers;
  - G. Electronic mail addresses;
  - H. Social security numbers;
  - I. Medical record numbers;

- J. Account numbers;
  - K. Certificate/license numbers;
  - L. Vehicle identifiers and serial numbers, including license plate numbers;
  - M. Device identifiers and serial numbers;
  - N. Web universal resource locators (URLs), also known as websites, which could be of either a personal or professional nature and relating directly to a client;
  - O. Internet protocol address numbers;
  - P. Biometric identifiers, including finger and voice prints;
  - Q. Full face photographic images and any comparable images; and/or
  - R. Any other unique identifying number, characteristic, or code.
- S. **Investigation**: A detailed inquiry or systematic examination; the process of inquiring into or following up; research; study; inquiry.
- T. **Intervention**: Interference so as to modify a process or situation; the act or fact of interfering with a condition to modify it or with a process to change its course.
- U. **Minimum Necessary** – The Covered Entity must make reasonable efforts to limit the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose of the use, disclosure, or request for data.
- V. **Outguide** – 9-1/2 by 12 inch plastic sheet with a plastic tab that says “out” on it. The plastic sheet has a clear pocket attached to it. The pocket holds a small piece of paper. The paper will state the name of the client whose chart has been pulled, the name of the employee who borrowed the chart, and the date the chart was borrowed.
- W. **Payment** – Activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- X. **Personal Representative** – A person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor; or the parent, guardian, or other person acting *in loco parentis* who is authorized except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service; or where the parent, guardian or person acting *in loco parentis* has consented to an agreement of confidentiality between the provider and the minor.
- Y. **Protected Health Information (PHI)** – Individually identifiable information that is maintained or transmitted that:
1. Is created or received by a covered entity, public health authority, employer, life insurer, school, or university;
  2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and
  3. Identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Patient/client identifying information which may not be disclosed without a consent includes, but is not limited to:

- 
1. Names
  2. Geographic subdivisions smaller than 20K
  3. Date of Birth other than year
  4. Telephone or fax numbers or E-mail addresses, URLs or IP addresses
  5. Social security numbers
  6. Medicare record numbers
  7. Health plan numbers
  8. Account numbers
  9. Certificate numbers
  10. Vehicle identifiers
  11. Device identifiers
  12. Biometric identifiers (finger or voice prints)
  13. Photographic images and the like
  14. Any other unique characteristic
- Z. **Public Health Authority:** An agent or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe; a person or entity acting under a grant of authority from or in contract with such a public agency, including:
- i. The employees or agents of that public agency;
  - ii. Its contractors or persons or entities to whom it has granted authority; and
  - iii. That is responsible for public health matters as part of its official mandate (45CFR, section 164.501).
- AA. **Security** – Ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. Under HIPAA this includes administrative procedures (access control, contingency planning), physical safeguards, technical security, and network security measures (internet, dial-in lines etc.).
- BB. **Surveillance:** A type of observational study that involves continuous monitoring of disease occurrence within a population.
- CC. **Transaction** – Under HIPAA, this is the exchange of information between two parties to carry out financial or administrative activities related to health care.
- DD. **Treatment** – The provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- EE. **Workforce Members** – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the department, its office, programs or facilities, is under the direct control of the department, office, program or facility, regardless of whether they are paid by the entity.

# **101-RM Initiation and Maintenance of Client Health Records**

## **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Initiation and Maintenance of Client Health Records
<b>ORIGINAL DATE ADOPTED:</b>	6/1/1992
<b>REFERENCE NUMBER:</b>	<b>101-RM</b>

## **PURPOSE**

The intent of this section to establish policies regarding the initiation and maintenance of client health records, regardless of the media on which they are stored. Media may include, but are not limited to hardcopy, electronic, microfilm, microfiche, and/or photographic forms.

## **PROCEDURES & STANDARD OPERATING GUIDELINES**

### **I. CLIENT HEALTH RECORDS**

The client health record is the property of Columbus Public Health. A designated employee in each program is responsible for the release of protected health information from the client health record.

A. The client health record may include, but is not limited to, the documents listed below:

1. Registration / identification information;
2. Admission agreements, consents, authorizations;
3. Referral information (records from other providers if referred for care);
4. History and evaluations, care plans, problem lists;
5. Service reports, contact forms, progress notes;
6. Discharge note, summary;
7. Release of information;
8. Privacy Notice acknowledgement.

Certain programs may also have additional record policies for compliance with accreditation standards. Please refer to the appropriate program manager for a more detailed list.

B. General documentation guidelines for legal purposes include:

1. Only authorized CPH staff members may make entries in the client health record.
2. Each page or screen in the client health record must be identified with the client's name and/or health record number.
3. Entries must be made in the client health record as soon as possible after the observation or event occurred.
4. Entries must indicate the actual date (month, day, and year) when each entry was made, as predating and postdating are both unethical and illegal.
5. Entries must include all pertinent facts relating to the observation or event being described.
6. Any change in the client's condition and all significant treatment issues must be noted until either the client stabilizes or the treatment issue is resolved, and documentation must provide evidence of follow-through.
7. If countersignatures are required by state regulations, only qualified staff member must countersign those entries.

8. The language used in the entries must be specific, factual, and objective, as opinions and speculations must not be included.
9. Only approved abbreviations will be allowed in the documentation. (See policy and procedure on approved clinical abbreviations at CPH).
10. Handwritten entries must be legible and written in permanent ink.
11. Entries in hardcopy records must be continuous with no gaps or extra spacing between entries, and blank lines in forms must be crossed out.
12. All applicable data fields on assessments, flowsheets, and checklists must be completed even when one or more of the fields does not apply to the client, so dashes or the abbreviation "NA," which stands for "not applicable" may be used in the blanks to prevent tampering.
13. Any conflicts or contradictions between entries must be addressed at the point of discovery.
14. The health record must contain evidence of the client's informed consent for treatments and procedures.
15. All communications and attempts at communication with the client, the client's significant others, and the client's other healthcare providers must be documented.
16. CDH staff with oversight responsibilities over other staff, students, or interns must ensure the consistency and completeness of all entries made by those staff individuals; the facts regarding adverse incidents must be documented in the progress notes, but there is to be no notation of an incident report anywhere in the health record.
17. Authors of any documentation must create and sign their own entries in both paper-based and electronic health record systems, and authors must never create or sign entries on behalf of another author. If electronic health record systems allow amendment or deletion of records, those systems should be reviewed as to levels of permission to alter the record.
18. Entries must contain only the documentation that pertains to the direct care of the client, and no personal statements or complaints will be entered.
19. If it is necessary to refer to another client when describing an event, that other client's health record number will be used in place of his/her name.
20. Corrections to entries in the client record are made by drawing a single line through the incorrect entries indicating "error" and writing the correct information, date and the author's initials near the original incorrect entry. Placing a new documentation entry over an existing one, scratching through the erroneous entry or using correction fluid ("white out") is not permitted. For corrections of electronic medical records, please refer to the appropriate electronic medical record system manual.
21. Late entries must include the time and date the late entry was entered into the health record, not the date that the entry should have been made.
22. Health records must never be removed from CPH except for client care reasons or in response to a legitimate court order or subpoena.

# **102-RM Safeguarding Protected Health Information (PHI)**

## **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Safeguarding Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>102-RM</b>

## **PURPOSE**

The intent of this section is to define appropriate guidelines to maintain the confidentiality and security of all protected health information (PHI) maintained by Columbus Public Health.

## **PROCEDURES & STANDARD OPERATING GUIDELINES**

### **I. SAFEGUARDING PROTECTED HEALTH INFORMATION**

- A. Columbus Public Health's clients are entitled to have the privacy of their health information protected, regardless of the form (hardcopy or electronic) in which that information is stored. Therefore, the department and its personnel have a responsibility to safeguard and ensure the confidentiality of the protected health information in the department's possession. Controls are required so that the protected health information is available for documentation, communication between personnel, billing, evaluation, education, research, and/or legal evidence whenever the need may arise. The protected health information will be protected against loss, defacement, tampering or use by unauthorized individuals.
- B. Columbus Public Health must make reasonable efforts to limit the access of its employees to protected health information. Therefore, Columbus Public Health must identify those employees or classes of employees who need access to protected health information to carry out their duties. In addition, for each such employee or class of employees, Columbus Public Health must define the category or categories of protected health information to which access is needed and any conditions appropriate to such access.
- C. Students who are assigned to/affiliated with the department for clinical/learning experiences and are providing supervised services to clients may have access to those clients' protected health information without the written consent of the clients (or legal guardians, if applicable). All individuals that have access to protected health information must sign a confidentiality agreement.
- D. Protected health information is not removed from the department premises except by court order or subpoena or as required for client visits or service documentation. This includes protected health information in any form, hardcopy or electronic, and stored in any manner (laptops, flash drives, floppy disks, etc.).
- E. The department must have in place reasonable safeguards to protect the privacy of protected health information from any intentional or unintentional use or disclosure that is in violation of HIPAA standards, implementation specifications, or any other requirements of HIPAA.
- F. Computer screens near public areas are to be rendered unreadable by special screen filters to avoid viewing by unauthorized individuals. Department employees' conversations regarding clients are to be of a professional nature only and must be conducted out of the earshot of unauthorized individuals.

- 
- G. Protected health information is to be kept in secured areas not accessible to the public. Protected health information is not left unattended in areas accessible to unauthorized individuals.
  - H. Protected health information removed from its storage area for treatment, review or administrative purposes is signed out whenever possible and returned as soon as possible. An out-guide, indicating when the protected health information was removed and for whom, should be filed in its place and removed upon return of the protected health information.

## **201.1-RM Confidentiality Policy**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Confidentiality Policy
<b>ORIGINAL DATE ADOPTED:</b>	7/2/2003
<b>REFERENCE NUMBER:</b>	<b>201.1-RM</b>

### **PURPOSE**

The intent of this section is to define Columbus Public Health's confidentiality guidelines.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

- A. Any record that contains a client's protected health information must be treated as strictly confidential and must be protected from loss, tampering, alteration, destruction, access, and unauthorized or inadvertent disclosure. Appropriate administrative, technical and physical safeguards must be maintained to protect access to a client's protected health information.
- B. Employees, interns, and volunteers must be informed about the importance of maintaining confidentiality of a client's protected health information during program orientation. The Confidentiality Agreement must be signed by employees, interns, and volunteers prior to starting duties and annually thereafter. The agreements will be maintained in the Human Resources office.
- C. All employees, interns, and volunteers are required to follow all CPH HIPAA policies and procedures.
- D. Health records (paper, microfilm, and electronic) are the property of CPH. The information contained in the records belongs to the client.
- E. CPH employees are obligated to use, disclose or request only the minimum amount of a client's protected health information that is necessary to accomplish the intended purpose of the use, disclosure or request. Employee access to a client's protected health information must be limited to only that health information that is needed to carry out his/her job duties.
- F. Access to work areas which have a client's protected health information are restricted to authorized CPH employees and individuals. Employees will prevent unauthorized disclosure of protected health information by restricting inappropriate access to computer terminals, work areas and identification codes. Computer user identification codes are confidential and not to be shared with others. Work areas and computers should be secured at all times.
- G. All employees are responsible for restricting the release of clients' protected health information. Written requests, as well as subpoenas and court orders, should be routed to these employees. These persons should verify proper authorization and process all requests for information.
- H. Each program shall have designated employees authorized to release clients' protected health information under strict conditions.
- I. Written requests, as well as subpoenas and court orders, should be routed to these employees. These persons should verify proper authorization and process all requests for information.

## **202.1-RM Authorization to Release Protected Health Information (PHI)**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Authorization to Release Protected Health Information (PHI)
<b>ORIGINAL DATE ADOPTED:</b>	3/11/2003
<b>REFERENCE NUMBER:</b>	<b>202.1-RM</b>

### **PURPOSE**

The intent of this section is to instruct all Columbus Health Department programs and employees regarding the use and disclosure of protected health information, and necessary authorization for such use or disclosure, as permitted or required by law.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. AUTHORIZATION TO RELEASE PHI**

- A. All uses and disclosures of protected health information beyond those otherwise permitted or required by law require a signed authorization.
- B. Unless required by law, patient/client identifying information may not be disclosed without authorization. This includes, but is not limited to:
  - 1. Names
  - 2. Geographic subdivisions smaller than 20K (zip codes)
  - 3. Date of Birth other than year
  - 4. Telephone or fax numbers or e-mail addresses, URLs or IP addresses
  - 5. Social security numbers
  - 6. Medical record numbers
  - 7. Health plan numbers
  - 8. Account numbers
  - 9. Certificate or license numbers
  - 10. Vehicle identifiers
  - 11. Device identifiers
  - 12. Biometric identifiers (finger and voice prints)
  - 13. Photographic images and the like
  - 14. Any other unique characteristic or code
- C. **Authorization Form:**
  - 1. All Columbus Health Department programs shall use the approved authorization form, as appropriate.
  - 2. If the authorization form does not meet a program's needs, the program shall draft a revision with a justification, and submit to the Privacy Officer/Committee.
  - 3. Only information permitted by the patient/client shall be released.
  - 4. The authorization to release information shall be signed by an adult, parent, guardian, or competent minor.

5. The “witness” can be anyone known by the patient/client or agency staff who witnesses the signature. A Notary Public is not necessary.
6. All of the following items must be present for the release to be valid.
  - i. Client name
  - ii. Date of birth or social security number
  - iii. Agency or person to whom the information is to be released
  - iv. Agency &/or program releasing the information
  - v. Type of information requested
  - vi. Purpose or need for information
  - vii. Revocation statement (request can be cancelled at any time)
  - viii. Redisclosure statement (prohibiting recipient from releasing the information further without written consent of the person to whom it pertains)
  - ix. Expiration date, or event or condition upon which release expires (such as termination of treatment)
  - x. Signature of client or authorized representative (such as parent, legal guardian, estate representative etc.)
  - xi. Witness signature
  - xii. Date signed
7. If any of the above items are missing, a valid release of information containing all of the above criteria **must** be obtained pursuant to the release of any information.
- D. The authorization must be retained for a minimum of six years.
- E. Information released to authorized individuals/organizations is strictly limited to the **minimum necessary** information required to fulfill the purpose on the authorization form. Requests that specify “any and all information” can either be returned for more specific information or satisfied with copies of pertinent portions of the record (i.e. history, assessment, orders, progress notes, summaries, test results, etc.).
- F. Photocopied authorization forms may be accepted but may also be deemed invalid if there appears to be tampering, changing, or defacement of any part of the form.
- G. An authorization form containing correction fluid (white out) or rubber stamp signatures will not be accepted.
- H. All information received from external health care and/or social service agencies maintained in the client record cannot be released unless the authorization is specifically stated to allow such release.
- I. The program shall contact a Columbus Health Department Health Information Manager when in doubt about an authorization to release information.
- J. Send a photocopy of the signed authorization to release information form to the client upon sending copies to the requestor.

## 202.2-RM Accounting for Disclosures of Protected Health Information (PHI)

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Accounting for Disclosures of Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	3/4/2003
<b>REFERENCE NUMBER:</b>	<b>202.2-RM</b>

### **PURPOSE**

HIPAA requires accounting for disclosures to be effective on April 14, 2002; the purpose of this section is to delineate for CPH staff how to account for disclosures of public health information.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. ACCOUNTING FOR DISCLOSURES OF PHI**

An individual has a right to receive an accounting of disclosures of protected health information (PHI) by Columbus Public Health during a time period specified up to a six (6) year period that began after April 13, 2003.

##### ***A. Exceptions (other than PHI maintained electronically as described below) to the accounting of disclosures include:***

1. Disclosures to carry out treatment, payment, and health care operations as permitted under law;
2. Disclosures to the individual about his/her own information;
3. Disclosures to persons involved in the individual's care, or other notification purposes permitted under law;
4. Disclosures pursuant to the individual's authorization;
5. Disclosures for national security or intelligence purposes;
6. Disclosures to correctional institutions or law enforcement officials as permitted under law;
7. Disclosures that occurred prior to April 14, 2003.

**NOTE: As of January 1, 2014 if the PHI is maintained in an electronic record:**

- B. Individuals have a right to receive an accounting of **all** disclosures of PHI during a time period specified up to a three (3) year period that began after January 1, 2014.
  1. This **includes** disclosures to carry out **treatment, payment, and health care operations** as permitted by law.
  2. This includes disclosures made by CPH's **business associates**, who must:
    - A. Present an accounting to CPH, who will in turn submit the accounting to the patient / personal representative; or
    - B. Respond **directly** to the patient / personal representative if directly contacted by the patient / personal representative.

#### **II. PROCEDURE FOR DISCLOSURE OF PHI**

- 
- A. **In the case of non-electronic records disclosures**, CPH programs must use the categories in the “Accounting for Disclosures Log” form, and may add other categories as needed.
  - B. The “Accounting for Disclosures Log” forms may be stored on paper or electronically. Backup needs to exist if stored electronically.
  - C. The “Accounting for Disclosures Log” for adults must be retained for six (6) years from last disclosure date on the log.
  - D. The “Accounting for Disclosures Log” for children and youth must be retained until the child is age 21 plus six (6) years from the last disclosure date on the log.
  - E. The individual’s request for an accounting must be acted upon no later than sixty (60) days after receipt of the request. If unable to provide the accounting within sixty (60) days, the time for response may be extended by no more than thirty (30) additional days provided that within the first sixty (60) days, the individual is given a written statement of
    1. The reasons for the delay;
    2. The date by which the accounting will be provided, and;
    3. There are no additional extensions of time for response.
  4. The first accounting in any twelve (12) month period must be provided to the individual without charge. A reasonable, cost-based fee may be charged for additional accountings within the twelve month period, provided the individual is informed in advance of the fee, and is permitted an opportunity to withdraw or amend the request. Staff should follow their program’s procedure regarding assessing fees for copies and the fee collection site.
  5. For disclosures from **electronic records**, an **electronic copy** of the patient’s health record must be provided if specifically requested in that format by the patient / personal representative.

## **202.3-RM Minimum Necessary Use of Protected Health Information (PHI)**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Minimum Necessary Use of Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	1/22/2003
<b>REFERENCE NUMBER:</b>	<b>202.3-RM</b>

### **PURPOSE**

The intent of this section is to issue instructions regarding Columbus Public Health's (CPH) responsibility relating to the HIPAA requirement to use, disclose or request only the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose.

This standard is applicable when using, disclosing or requesting PHI from another Covered Entity.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. MINIMUM NECESSARY USE OF PHI**

CPH will make reasonable efforts to ensure that the minimum necessary PHI is disclosed, used, or requested. Exceptions include disclosures:

- A. To the individual who is the subject of the information;
- B. Made pursuant to a valid authorization requested by the individual;
- C. To healthcare providers for treatment purposes;
- D. Required for compliance with the standardized HIPAA transactions;
- E. Made to the Department of Health and Human Services pursuant to a privacy investigation;
- F. Otherwise required by the HIPAA regulations or other law.

#### **II. MINIMUM NECESSARY USE PROCEDURE**

The following procedures will be implemented to ensure that this policy is enforced effectively across all divisions.

- A. Each CPH classification/position having access to PHI will be identified. The category(s) of PHI to which access is needed and any conditions appropriate to such access will be established. Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties.
- B. For situations where PHI disclosure occurs on a recurring basis, the PHI disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the disclosure.
- C. Requests for multiple disclosures will be reviewed by CPH's HIPAA Steering Committee. Information disclosed will be limited to that which is reasonably necessary to accomplish the purpose for which disclosure is sought.
- D. All CPH employees will be trained regarding this policy. New employees will be trained during the employee orientation.
- E. Questions regarding these procedures should be directed to CPH's Privacy Officer/Committee. All CPH employees will be trained regarding this policy. New employees will be trained during the employee orientation.

## **202.4-RM Notice of Privacy Practice**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Notice of Privacy Practice
<b>ORIGINAL DATE ADOPTED:</b>	3/4/2003
<b>REFERENCE NUMBER:</b>	<b>202.4-RM</b>

### **PURPOSE**

The intent of this section is to instruct all Columbus Health Department programs about issuing the Columbus Public Health Privacy Notice to all clients.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. NOTICE OF PRIVACY PRACTICE**

In compliance with 45 CFR 164.520; a client, excluding an inmate of a correctional facility, has the right to be informed about:

1. How Columbus Public Health uses and disclosures the client's PHI.
2. Columbus Public Health's responsibilities with respect to the use of the client's PHI.

##### **A. *Columbus Public Health will:***

1. Promptly revise and distribute the most current form of the Privacy Notice when any change is made.
2. Maintain a copy of the notice in the Health Commissioner's Office for a period of six years from the date it was last in effect.
3. Prominently post the current version of the Privacy Notice in effect and have copies available for clients at all service delivery sites, and on Columbus Public Health's website.

##### **B. *Every Columbus Health Department Program will:***

1. Post and distribute the most current Privacy Notice.
2. Provide clients with the Privacy Notice and obtain the client's written acknowledgement of this notice on the first date of service or, for established clients, on the first day of service on or after April 14, 2003.
3. Maintain copies of the Receipt of Privacy Notice in the client's chart for a period of at least six years from the date signed.

# **203-RM Disclosure of Client Information Regarding HIV Testing or Treatment**

## **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Client Information- HIV Testing or Treatment
<b>ORIGINAL DATE ADOPTED:</b>	6/1/1992
<b>REFERENCE NUMBER:</b>	<b>203-RM</b>

## **PURPOSE**

The intent of this section is to establish policies and procedures that will protect individually identifiable information pertaining to the results of HIV tests and/or HIV treatment from unauthorized or inadvertent disclosure in accordance with Section 3701.243 of the Ohio Revised Code (ORC).

## **PROCEDURES & STANDARD OPERATING GUIDELINES**

### **I. DISCLOSING WRITTEN CLIENT HIV MEDICAL INFORMATION WITHOUT INFORMED CONSENT**

The results of an HIV test or the identity of an individual on whom an HIV test is performed may be disclosed WITHOUT informed consent and without a signed authorization to release information in the following situations:

- A. Verbally in person to the individual client who was tested after verification of identity using the appointment slip with the opscan number and/or picture identification;
- B. Written confirmation of positive HIV test results are reported by Columbus Public Health's Sexual Health Program performing the test to the Ohio Department of Health (ODH) as required by 3701.24 ORC;
- C. Written or verbal summary reports generated by Columbus Public Health's programs, minus individual client identifiers, can be released to Columbus Public Health's committees responsible for quality assurance, patient care evaluation, service or program reviews and management of financial audits;
- D. Summary reports, minus individual client identifiers, in writing to accrediting or licensing agencies or oversight review organization as required for certification or accreditation purposes;
- E. Written results to law enforcement authorities pursuant to a search warrant or a court order issued specifically for HIV test results by or at the request of a grand jury, a prosecuting attorney, the city director of law or a similar chief legal officer of a municipal corporation or village. For subpoenas, please refer to the 209-RM, the Policy and Procedure for Responding to a Subpoena or Court Order;
- F. To a health care facility that procures, processes, distributes, or uses a human body part from a deceased client to ensure that the body part is medically acceptable for its intended use;
- G. To a health care provider, emergency medical services worker, or peace officer who sustained a significant exposure to the body fluids of a client if the client was tested pursuant to division (E)(6) of section 3701.242[3701.24.2]of the ORC, except that the identification of the client shall not be revealed;
- H. To a health care provider, if the provider has a medical need to know the information and is participating in the diagnosis, care or treatment of the client on whom the test was performed or who has been diagnosed as having the HIV virus, AIDS, or an AIDS-related condition;
- I. If CPH considers it necessary to disclose the results of an HIV test of a specific client in an action in which CPH is a party, CPH may seek authority for the disclosure by filing an in camera motion with the court in which the action is being heard;

- 
- J. In a civil action in which a plaintiff seeks to recover damages from a client based on an allegation that the plaintiff contracted the HIV virus as a result of actions of the client, the prohibitions against disclosure in ORC 3701.243 do not bar the discovery of the results of any HIV test given to the client or any diagnosis that the client suffers from the HIV virus, AIDS, or an AIDS-related condition.

**II. DISCLOSING WRITTEN CLIENT HIV MEDICAL INFORMATION**

- A. Please see the Policy and Procedure for Processing of Written Requests for Protected Health Information.
- B. Prior to sending the photocopies of the record, stamp the following statement on each photocopy page OR send a cover letter to the requesting party with the following statement included:

*“This information has been disclosed to you from confidential records protected from disclosure by state law. Ohio Revised Code 3701.24 prohibits you from making any further disclosure of it without the specific, informed consent of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of HIV test results or related diagnoses is not sufficient for the purpose of the release of HIV test results or diagnoses.”*

## 204-RM Disclosure of Client Information Regarding Drug and Alcohol Abuse Programs

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Client Information- Drug and Alcohol Abuse Programs
<b>ORIGINAL DATE ADOPTED:</b>	6/1/1992
<b>REFERENCE NUMBER:</b>	<b>204-RM</b>

### **PURPOSE**

The intent of this section is to establish policies and procedures that will protect records of clients in accordance with 42 CFR Part 2 and HIPAA from any unauthorized or inadvertent disclosure. This protection is extended to those individuals who have been identified for prevention services or to those who have been diagnosed and/or treated in a drug and alcohol abuse program, past or present.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. DISCLOSING CLIENT INFORMATION FOR DRUG AND ALCOHOL ABUSE**

A program is defined by law as “an individual, partnership, corporation, Federal, State or local government agency, or any other legal entity which receives federal assistance and in whole or in part holds itself out as providing alcohol or drug abuse prevention, diagnosis, treatment or referral for treatment. A health care facility can be a “program” if it has:

- A. “A(n) identified unit that provides alcohol or drug abuse diagnosis, treatment or referral for treatment; OR
- B. Medical personnel or other staff whose primary function is the provision of alcohol or drug abuse diagnosis, treatment, or referral for treatment and who are identified as such providers.”
- C. Statutes and rules regarding confidentiality of client records are intended to ensure that a client in an alcohol or drug abuse or prevention program is not made more vulnerable by reason of the availability of his or her client record, than an individual who has an alcohol and drug abuse problem and does not seek treatment.
- D. Program staff shall not confirm or deny to any persons or entities outside of the program that a client attends or receives services from the program. Additionally, program staff shall not disclose any information identifying a client as an alcohol or other drug services client unless:
  1. The client consents in writing for the release of the information;
  2. The disclosure is allowed by a court order;
  3. The disclosure is made to qualified personnel for a medical emergency, research, audit or program evaluation purposes.
- E. Federal laws and regulations do not protect any threat to commit a crime, nor any information about a crime committed by a client either at the program or against any person who works for the program.
- F. Federal laws and regulations do not protect any information from being reported under state law to appropriate state and local authorities when it pertains to suspected or known child abuse or neglect.
- G. Protected client information includes any information or records, recorded or not, relating to a client and any client identifying information including, but not limited to name, address, social security number, driver’s license, and / or numbers assigned by the program or service providing care.
- H. The client records to which the statute and regulations apply may be disclosed or used only as permitted by these regulations and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceeding. The use of any client information to initiate or substantiate any criminal charges against a client or

to conduct any criminal investigation of a client is prohibited. This includes information on diagnosis, treatment or referral for treatment.

- I. Restrictions on disclosure and use apply whether the holder of the information believes that the person seeking the information already has it, has other means of obtaining it, is a law enforcement official, has obtained a subpoena, or asserts any other jurisdictional reason for disclosure.
- J. If a person is not now and never has been a client, there is no client record and these restrictions do not apply.
- K. Any answer to a request for disclosure of client information which is not permissible must be made in a way that will not affirmatively reveal that an identified individual has been, or is being treated for alcohol or drug abuse. An inquiring party may be given a copy of the regulations and may be advised that they restrict disclosure of alcohol and drug abuse client records, but may not be told affirmatively that the regulations restrict the disclosure of the records to an identified client.

## **II. DISCLOSING CLIENT INFORMATION WITHOUT WRITTEN CONSENT**

### **A. *Disclosure without Written Consent***

Disclosure without written consent should only occur in the following types of situations. If you are unsure whether to release information, always consult your program manager for guidance.

- 1. When medical personnel who have a need for information about the client for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention.
- 2. Upon the issuance of a subpoena accompanied by a court order from a court of competent jurisdiction. A subpoena alone is not sufficient means for automatic disclosure.
- 3. Immediately following disclosure, the responsible person must document the disclosure in the client's record. This information must include:
  - i. The name of the medical personnel to whom the disclosure was made;
  - ii. The name of the individual making the disclosure;
  - iii. The date and time of the disclosure; AND
  - iv. The nature of the emergency.

### **B. *Disclosure with Written Consent***

Upon receipt of a written authorization to release information:

- 1. Mark the date received on the request.
- 2. Verify the client as one having been seen by the program. If the person is not now and never has been a client, so notify the requesting party. If additional information is necessary to identify the client, the requesting party is notified.
- 3. Review the authorization for compliance with legal guidelines. If the authorization does not contain all the necessary provisions, the requesting party is informed. If the authorization is not valid, a CPH Alcohol and Drug Abuse Program authorization to release information form is sent to the requesting party.
- 4. Locate the client's record and photocopy ONLY the requested information after verifying applicable signatures/authority to sign.
- 5. Stamp the following statement on each photocopied page OR send a cover letter to the requesting party with the information. The statement must be similar to the following:

*"This information has been disclosed to you from records whose confidentiality are protected by Federal law. Federal Regulations (42 CFR Part 2) prohibit you from making any further disclosure of it without the specific, written, informed consent of the person to whom it pertains."*

- 
6. Complete the cover letter indicating the date the information was sent, to whom it was sent, who prepared the copies, and a listing of the record page copies sent.
  7. Send the information and a letter to the requesting party.
  8. File a copy of the letter, the original authorization form, and the request letter in the client's record for future reference. Record the action in a progress note. If no record is available, record information about this transaction in the HIPAA Log.

## **209-RM Responding to a Subpoena or Court Order**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Responding to a Subpoena or Court Order
<b>ORIGINAL DATE ADOPTED:</b>	6/1/1992
<b>REFERENCE NUMBER:</b>	<b>209-RM</b>

### **PURPOSE**

The purpose of this section is to provide guidelines regarding when a Columbus Public Health medical record is subpoenaed.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

Protected health information written during the normal course of business at Columbus Public Health can be admitted into evidence in a court of law only through the legal processes described below. Employees should become familiar with the definitions and procedures described below in order to facilitate a proper response when subpoenas and/or court orders are received.

#### **I. THE COURT ORDER**

Under normal circumstances, before a trial begins, CPH initially receives a request from an attorney for copies of protected health information to be used in the attorney's preparation for a case. If a dispute arises about whether the protected health information released for use can be used as evidence at the trial, or if there are other objections related to the protected health information, the issue must be resolved by the court.

When this occurs, CPH may receive a command, known as a "court order," from the court involved, directing CPH to submit the protected health information to all attorneys involved in the case. Court orders, which can be issued by a federal, state, county or municipal court, are usually issued in written form. However, a judge may also make court orders verbally to CPH. In either event, CPH must comply with the court order.

CPH may, upon consultation with the city attorney's office, have reason to believe that it should not submit the protected health information demanded by the court. If so, CPH may contest the order, but it may not refuse to comply. Once the court issues a final and legal order, CPH must comply or face a contempt-of-court citation.

For alcohol and drug records, please refer to 42 CFR, Part 2.

#### **II. THE SUBPOENA**

A subpoena is a written request by one of the parties involved in the litigation, issued by the authority of the court, to compel a witness to appear and give testimony or provide protected health information. When a witness is subpoenaed, he/she may be commanded to appear at either a trial or a deposition, a pre-trial procedure in which the court allows the parties to a legal action to obtain information which might settle the action before trial, simplify issues, or aid the attorneys in preparing their cases.

CPH may receive one of two types of subpoenas:

- A. *Subpoena ad testificandum*, which requires a person to appear and present oral testimony ONLY.

- B. *Subpoena duces tecum*, which requires a person to appear and present testimony at a trial or other proceeding AND/OR bring all documents and records as specified in the subpoena.

Subpoenas for protected health information must be accompanied by either an authorization signed by the client or his/her personal representative OR a valid court order.

### **III. RESPONSE PROCEDURE**

- A. Verify the validity of the subpoena or court order. It must cite:
1. Name of the court (civil, criminal, municipal, etc.);
  2. Name of the health care facility/program/person subpoenaed (i. e., Columbus Health Department, Ben Franklin Clinic, staff member John Doe);
  3. Case docket number;
  4. The names of the plaintiff and defendant;
  5. The date, place and time of the required appearance or submission of records;
  6. The name and phone number of the person (attorney or judge) who is requesting you to appear;
  7. The specific documents sought (duces tecum);
  8. Signature or stamp and seal of the official who issued the subpoena or court order.
  9. Contact the attorney who issued the subpoena to obtain complete client identifying information, including date of birth and social security number.
- B. Verify whether your program has possession of the record being subpoenaed. If your program does not have the records, contact the party issuing the subpoena in writing and inform them of this.
- C. Notify the attending physician, case manager and/or program director that a subpoena or court order has been received.
- D. Fax to the city attorney's office the subpoena or court order for determination of validity. If only a subpoena is received, request a consultation with the city attorney regarding the need for either:
1. Additional authorization from the client or his/her personal representative to release the protected health information; OR
  2. A court order; OR
  3. The submission of written objections by the city attorney to production of the protected health information.
- E. Threats and intimidation from the requestor should be reported to the city attorney's office immediately.

If the court determines that the subpoena requires disclosure of privileged or otherwise protected information *and no exception or waiver applies*, the court can quash or modify the subpoena, or the court can order the production of the protected health information under specified conditions (Ohio Civ. R. 45 (C) (2) (b) and 45 (C) (3) (b)).

*Note:* For cases involving custody rights (child or adult) or clients with known mental or chemical dependency problems, a court order will be required.

- F. If only a subpoena is presented and neither a court order nor a valid, signed authorization from the client or his/her personal representative is forthcoming, one of the following documents must be presented to the CHD before the protected health information can be presented in court:
1. The CHD must receive satisfactory assurances in writing from the party seeking the information

that reasonable efforts have been made by that party to ensure that the individual who is the subject of the information has been given notice of the request.

In this case, "satisfactory assurances" means a written statement and accompanying documentation demonstrating that:

- i. The party requesting the information has made a good faith attempt to provide written notice to the client;
- ii. The notice to the client contained enough information to permit the client to raise an objection to the court; AND
- iii. The time for the client to raise objection to the court has elapsed and either no objections were raised or all objections raised have been resolved.

2. The CHD must receive satisfactory assurances from the party seeking the information that reasonable efforts have been made by that party to secure a qualified protective order from the court.

In this case, "satisfactory assurances" means a written statement and accompanying documentation that:

- i. All parties to the dispute in court giving rise to the request for information have agreed to a qualified protective order and have presented the order to the court; OR
- ii. The party seeking the protected health information has requested a qualified protective order from the court.

*Note:* A "qualified protective order" means an order of the court or a stipulation by the parties to the litigation that:

- i. Prohibits the parties from using or disclosing the information for any purpose other than the litigation or proceeding for which such information was requested; AND
- ii. Requires the return to the CHD or the destruction of the information (including all copies made) at the end of the litigation or proceeding.

G. Also, according to Section 164.512 (e) (1) (vi), the CHD may disclose protected health information in response to a subpoena without receiving satisfactory assurances from the parties if the CHD:

1. Makes a good faith attempt to provide written notice to the client; OR
2. Makes reasonable efforts to seek a qualified protective order.

H. Thus, if the CHD receives a subpoena without any accompanying documents, the CHD can do one of two things:

1. It can serve a written objection upon the attorney/party who issued the subpoena because the information sought is protected health information, and the subpoena was not accompanied by a court order, an authorization from the client or his/her personal representative, or qualified protective order from the court; OR
2. It can contact the attorney/party issuing the subpoena and inform him/her that the information requested is protected health information and is covered by HIPAA, which requires additional documents before protected health information can be presented in court. If the documents are not forthcoming, CHD will serve a written objection on the attorney/party and allow the court to decide how to proceed.

I. Furthermore, the CHD will make the attorney/party aware, in writing, that:

1. Pursuant to HIPAA regulations, the parties are prohibited from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
  2. HIPAA regulations require the return of the protected health information (including copies) to the CHD at the end of the litigation or proceeding OR destruction of the protected health information.
- J. Verify control of the record using the information contained on the face of the subpoena or court order. Contact the attorney who issued the subpoena to obtain complete client identifying information (birth date, etc.) if needed.
- K. Contact the attorney who issued the subpoena to see whether certified copies of the protected health information may be sent in lieu of making a court appearance. If the attorney refuses to receive certified copies, verify the date and time the appearance is needed at the deposition, hearing or trial and ask to be placed "on call."
- L. Review the record to ensure that it is complete, the signatures are identifiable and each page of the record contains the client's name and identification number.
1. If the subpoena calls for other documents (i. e., bills) not normally contained in the record, obtain these.
  2. Review the record to make sure only those items *specifically requested* in the subpoena or court order are included.
- M. If the subpoena or court order specifically requests information originally generated by another provider and contained in the record, it should be included in the records that are prepared. The responsibility of determining admissibility of this information is that of the attorneys and the court.
1. Information that is *not specifically* requested should be removed before the record is released.
- N. If the attorney agrees to accept certified photocopies of the record:
1. Verify the completeness of the record;
  2. Do not make any alterations in the record or allow anyone else to make additions, corrections, or deletions after the subpoena/court order has been received;
  3. Number the pages (bottom right corner) in ink. If a page is completed on both sides, number each side;
  4. Prepare the photocopies (both sides of two-sided forms);
  5. Make a record of what has been copied and place it in the medical record.

#### **IV. FOR COPIES OF RECORDS MAILED IN LIEU OF APPEARANCE**

- A. Obtain a notarized certification statement. According to Section 2317.422 of the Ohio Revised Code, the certification statement must accompany the record copies.
- B. Mail or deliver the certified copies of the record to the Clerk of Courts for the court that is hearing the case. Copies must be received no less than FIVE days before the trial. The Clerk of Courts will then mark the records as evidence and forward a copy to the respective lawyers handling the case.
  1. Place all the copies and the certification statement in an envelope with the following information on the face of the envelope:
    - i. Name of the court;

- ii. Case number
2. Mail the copies by registered mail or deliver them with a return receipt requested.

**V. IF TESTIFYING AND DELIVERING THE RECORD IN PERSON**

- A. Make an exact copy of the entire record, as described in Processing of Subpoena. Certify the copies using the Certification of Records Custodian Form in case testimony is not required upon your arrival at court.
- B. Make yourself familiar with the record before going to court. Make sure you can identify signatures, names, dates, etc.
- C. Take the copies and the original record to court. Make an additional copy to keep in the record file while you are outside the building with the record. Occasionally, the court will direct you to leave the original record as evidence. However, whether an original or a copy is left with the court or the attorneys, you must obtain the recipient's signature on the Court Receipt for Records form (see attached). Maintain a copy of the receipt and inventory for your files and follow up with the Clerk of Courts until either the original record is returned or the copies are returned or destroyed.
- D. When you arrive at court, report to the bailiff so that he/she can make a note of your presence. Also, seek out the opposing attorneys, and in their presence, ask them if they will stipulate the entry of the records as copied. If they both agree, this may eliminate the need for you to testify.
- E. If either attorney disagrees to stipulating the records and you have to testify, be sure that you do not release any records until you are asked to do so on the stand. Never let just one of the attorneys review the record unless you are on the stand or the opposing attorney is also present.
- F. When testifying, be clear and concise. Only answer questions that you have knowledge of personally.
  1. The attorney will ask some identifying questions first to establish you as a credible witness. Most questions can be answered with a simple "yes" or "no" response. Don't be afraid to say, "I don't know."

**VI. AFTER RETURNING FROM COURT**

- A. Staple a note to the subpoena, which includes the following:
  1. By whom the subpoena was answered;
  2. Date and time of the court appearance;
  3. Attorneys' names;
  4. Specify whether the original record or a copy of the record was left with the court and/or either attorney.
- B. File the subpoena in the record folder until the original version of the record is returned.

**VII. AFTER THE ORIGINAL RECORD IS RETURNED**

- A. *Check the returned record against the record copy to make sure all the pages are present.*
- B. *Reassemble the original record in proper order, if necessary.*
- C. *On the note stapled to the subpoena, write the date the record was returned.*
- D. *File the record, the subpoena, the note and the court receipt together in the original record folder, and return the record to its proper place in the file.*

## **210-RM Confidentiality of Protected Health Information Via Facsimile (Fax) and Electronic Mail (Email)**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Confidentiality of Protected Health Information Via Facsimile (Fax) and Electronic Mail (Email)
<b>ORIGINAL DATE ADOPTED:</b>	6/1/1992
<b>REFERENCE NUMBER:</b>	<b>210-RM</b>

### **PURPOSE**

The intent of this section is to establish policies and procedures for Columbus Public Health that will protect the confidentiality of patient health information that is transmitted to and received from authorized parties.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. FAX AND EMAIL**

A valid client authorization must be obtained prior to release of protected health information. All CHD fax machines must be placed in secure locations to prevent unauthorized access or use.

Electronic transmission of client health information should be limited to urgent or non-routine health care purposes only. It is strongly recommended that routine disclosure of information to insurance companies, attorneys, or other legitimate users should be made through regular mail. The information transmitted should be limited to the minimum necessary.

##### ***A. Processing Outgoing Fax Transmittals***

1. The CPH fax cover sheet must precede the transmission of client health information. Documentation of the transmission must be maintained in the client's record or maintained in the program area after transmission. The cover sheet includes the following:
  - i. Sender's name and phone number
  - ii. Receiver's name and phone number
  - iii. Date of transmission
  - iv. Number of copies sent
  - v. Content of fax
2. Transmission of Fax
  - i. Verify the recipient of the fax and confirm that fax number is correct .
  - ii. Obtain printed confirmation of each outgoing transmission and/or request confirmation from recipient.
  - iii. Use speed-dial feature for routinely used fax numbers
  - iv. Verify that fax is being sent to a secure site, and notify the recipient when the fax is sent.
  - v. Assure that fax machine prints a confirmation of each outgoing transmission.

---

**B. Processing Incoming Fax Transmittals**

1. Ensure that fax machine is in a secure location.
2. Designated staff must check the fax machine at regular intervals for prompt retrieval and distribution of the faxes to the appropriate recipients.

**C. Misdirected Fax Transmissions**

1. If a fax transmission is received by the CHD in error, notify the sender of the information and destroy all materials.
2. If a fax transmittal from the CHD is sent in error to the wrong recipient:
3. Request that the fax be destroyed immediately.
4. Notify immediate supervisor if protected health information is involved.

**D. Email Transmissions**

1. Email must not be used for protected health information unless programs have encrypted email software.
2. Email access is for the purpose of facilitating work related functions only.
3. Email messages are confidential and may be accessed only by the recipient of the message.
4. Outgoing email messages will contain the following confidentiality statement:

**CONFIDENTIALITY NOTICE:** *This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.*

## 211-RM Business Associate Agreements

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Business Associate Agreements
<b>ORIGINAL DATE ADOPTED:</b>	3/21/2003
<b>REFERENCE NUMBER:</b>	<b>211-RM</b>

### **PURPOSE**

The intent of this section is to explain that all vendors and business partners who have access to protected health information must sign privacy agreements.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. BA AGREEMENT PROCEDURE**

- A. Business Associate (BA) Agreements must be signed by all vendors and business partners to whom Columbus Public Health will transfer confidential, personally identifiable health information or who have access to protected health information generated or received by Columbus Public Health.
- B. BA Privacy Agreements will be appended to all new contracts or memorandums of agreement (MOA), effective April 14th, 2003.
- C. BA Privacy Agreements will be maintained on file in the Fiscal Office, even when the contract/agreement is not financial.
- D. For those BAs with whom Columbus Public Health does not have a formal written contract or MOA but who are subject to privacy regulations, the Fiscal Office will ensure that a privacy agreement is signed by the BA once every fiscal year (process to be completed by January 31st of each year). These agreements will be filed in the Fiscal Office.
- E. BA Associate Privacy Agreements that are received by Columbus Public Health from external entities:
  - a. *If Columbus Public Health is the payor, the BA must sign Columbus Public Health's Privacy Agreement because it is the covered entity.*
- F. Requests from external entities will be handled as follows:
  1. The program manager in charge of the project or specific service determines if the request is valid, and if unsure (s)he will contact the Privacy Officer.
  2. If the request is *not* valid, the program manager will explain Columbus Public Health's policy to the external entity.
  3. If the request is valid, program manager in charge of the specific service or project, *signs and sends* the original agreement(s) to the Privacy Officer;
  4. Privacy Officer *signs* as a representative of the Health Commissioner, *returns originals* to program manager and *forwards a copy* to Fiscal Office
  5. Program Manager *returns signed original* to external entity.
  6. Fiscal Office *files copy*.

## **212-RM HIPAA Client Complaint Process**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	HIPAA Client Complaint Process
<b>ORIGINAL DATE ADOPTED:</b>	8/4/2003
<b>REFERENCE NUMBER:</b>	<b>212-RM</b>

### **PURPOSE**

The intent of this section is to investigate all complaints made by clients who believe their confidentiality rights under HIPAA have been violated.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. CLIENT COMPLAINT**

Columbus Public Health will investigate all complaints made by clients who believe their rights under HIPAA have been violated. These violations may occur either through a CPH employee's and/or business associate's failure to follow CPH's policies and procedures regarding HIPAA or through CPH's failure to follow the requirements of the privacy regulations established under HIPAA.

The following procedures will be implemented to ensure that this policy is enforced effectively across all divisions.

- A. Any CPH employee receiving a complaint (telephone, written, or personal) from a client or the client's personal representative involving the client's rights as listed in CPH's Privacy Notice will ask the client/personal representative to complete a complaint form. The employee will assist the client/personal representative in completing the form, if needed.
- B. The client/personal representative will submit the completed form to the employee. The employee will submit the complaint form within 2 working days to both the Privacy Officer and the supervisor of the work area involved in the complaint.
- C. The supervisor will:
  1. Initiate an investigation regarding the complaint within 2 working days.
  2. Report his/her findings and recommendations to the Privacy Officer within 5 working days via the complaint form.
- D. The Privacy Officer will:
  1. Send a letter to the client/personal representative within 2 working days of receiving the complaint, stating that the complaint has been received and is being investigated. In addition, the letter must state that the client/personal representative will be made aware of the conclusions reached in the investigation.
  2. Determine whether the client's rights have been violated within 10 working days.
  3. Inform the supervisor within 2 working days if a violation has occurred.
- E. If a violation has occurred the supervisor will:

---

Initiate progressive disciplinary action against the employee(s) responsible.

F. The Privacy Officer will:

1. Follow the guidelines set forth in the policy and procedure for Business Associate Agreements if a violation has been committed by CPH's business associates.
2. Communicate any liability issues and/or concerns regarding possible litigation to the City Attorney within 5 working days of receiving the supervisor's report via the complaint form.
3. Work with the City Attorney, if necessary, to plan for mitigation, to the extent practical, of any harmful effects that resulted from the unauthorized use/disclosure of the client's protected health information.
4. Communicate in writing with the client/personal representative regarding the outcome of the investigation within 30 days of the conclusion of the investigation.
5. Send a photocopy of the above communication to the supervisor.
6. Retain a photocopy of the above communication, along with the original complaint form and any other correspondence or documents regarding the investigation, for a period of six years.

G. In the event that the Privacy Officer is on leave, the Assistant Commissioner will assume the responsibilities of the Privacy Officer.

## 213-RM Release of Protected Health Information of Clients Experiencing Abuse, Neglect and/or Domestic Violence

### POLICY AND PROCEDURE

<b>SUBJECT/TITLE:</b>	Release of Protected Health Information of Clients Experiencing Abuse, Neglect and/or Domestic Violence
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>213-RM</b>

### PURPOSE

The intent of this section is to explain circumstances under which protected health information may be released when adult and minor clients are believed to be victims of abuse, neglect or domestic violence.

### PROCEDURES & STANDARD OPERATING GUIDELINES

CPH may disclose protected health information about adult and minor clients whom CPH reasonably believes to be victims of abuse, neglect and/or domestic violence. The following definitions are relevant to this section.

1. **Abuse** means all of the following (ORC 5123.50 and 5101.60):
  - i. The use of physical force that can reasonably be expected to result in physical harm or serious injury;
  - ii. The infliction of injury upon an adult by himself/herself or others, unreasonable confinement, intimidation, or cruel punishment with resulting physical harm, pain, or mental anguish;
  - iii. Sexual abuse, including unlawful sexual conduct or sexual contact; AND
  - iv. Verbal abuse, including purposely using words to threaten, coerce, intimidate, harass, or humiliate an individual.
2. **Neglect** means failing to provide an individual with any of the following that are necessary to maintain the health and safety of the individual when there is a duty to do so (ORC 5101.60):
  - i. Treatment;
  - ii. Care;
  - iii. Goods; OR
  - iv. Services.
3. **Domestic violence** means (ORC 3113.33):
  - i. Attempting to cause or causing bodily injury to a family or household member; OR
  - ii. Placing a family or household member in fear of imminent physical harm by threat of force.
4. **Exploitation** means the unlawful or improper act of a caretaker using an adult or an adult's resources for monetary or personal benefit, profit or gain (ORC 5101.60).
5. A **dependent child** means any child (ORC 2151.04):
  - i. Who is homeless or destitute or without adequate parental care, through no fault of the child's parents or guardian; OR
  - ii. Who lacks adequate parental care by reason of the mental or physical condition of the child's parents, guardian or custodian; OR
  - iii. Whose condition or environment is such as to warrant the state, in the interests of the child, in assuming the child's custody; OR

- iv. Who resides in a household in which a parent/guardian or other member of the household committed an act that was the basis for adjudication that another child residing in that same household is an abused, neglected or dependent child.

## **I. REPORTING ABUSE/NEGLECT/DOMESTIC VIOLENCE POLICY**

Such disclosures can only be made to agencies authorized by law to receive such reports, including:

- A. ***Social service or protective services agencies; AND***
- B. ***Authorized law enforcement officials.***

The disclosures must be made if there is reason to believe that there is a wound, injury, disability or condition which reasonably indicates that the abuse or neglect has occurred (ORC 2151.421, regarding child abuse, ORC 5101.61 regarding the abuse of elderly persons, and ORC 5123.61 regarding the abuse of adults with mental retardation or developmental disabilities.) All such disclosures will be documented in written form in the client's medical record.

Generally, the client or his/her personal representative must agree to the disclosure, or, ***in the absence of such an agreement:***

- A. CPH, in the exercise of professional judgment, must believe that the disclosure without agreement is necessary to prevent serious harm to the client or other potential victims;
- B. The client is unable to agree because of incapacity or inability; OR
- C. An authorized law enforcement official states that the law enforcement activity may be adversely affected by waiting until the client is able to agree to the disclosure.

If CPH chooses to make such a disclosure; it must promptly inform the client that such a report has been or will be made, ***except*** if CPH:

In the exercise of professional judgment, believes that informing the client would place the client at risk of serious harm; OR Has reason to believe that the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the client.

## **II. REPORTING ABUSE/NEGLECT/DOMESTIC VIOLENCE PROCEDURE**

All staff members who become aware of any situation of client *abuse* or *neglect* must:

- A. Bring this information to the immediate attention of a Program Manager, the Program Administrator or designee.
- B. Immediately contact the appropriate agency:
  - 1. The Columbus Police Department or the Franklin County Sheriff's Department in any situation that appears to involve criminal activity;
  - 2. Franklin County Children Services or the Columbus Police Department in situations involving minors/dependent children;
  - 3. Franklin County Adult Protective Services with regard to the abuse, neglect or exploitation of individuals aged 60 or over; OR
  - 4. Franklin County Board of Developmental Disabilities or the Columbus Police Department for situations involving developmentally disabled adults.

C. Within 72 hours of receiving the allegations:

1. Complete any documentation required by the above mentioned agencies; AND
2. Document all of the above in the client's medical record in the progress notes/service notes section.

D. All staff members who suspect domestic violence involving a client must bring this information to the immediate attention of a Program Manager or the Program Administrator or designee.

1. The staff member / designee will:
  - i. Provide information to the client regarding Choices for Victims of Domestic Violence, the Franklin County Municipal Court's Crime Victims Compensation Program, the Columbus Police and / or the Franklin County Sheriff.
  - ii. Document in the client's record any referrals made and any subsequent communication made to the agencies to whom the client was referred; AND
  - iii. Immediately report to Franklin County Children Services or the Columbus Police Department any domestic violence situations in which a child's safety appears questionable.

## 214-RM Personal Representatives' Role in the Release of Protected Health Information (PHI)

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Personal Representatives' Role in the Release of Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>214-RM</b>

### **PURPOSE**

The intent of this section is to explain circumstances under which individuals acting as personal representatives of clients may make protected health information disclosure decisions on clients' behalf.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. RELEASE TO PERSONAL REPRESENTATIVES**

CPH accepts that a personal representative may make health care decisions on behalf of a client when the client is incapable of doing so. This relationship must be based upon the execution of a legal document, such as a durable power of attorney for health care, or it may be based upon a parent-and-minor child relationship.

A. Individuals acting as personal representatives of a client and having the legal right to make health care decisions regarding a client may also make decisions regarding the client's protected health information. This includes individuals who can provide legal documentation that they are:

1. Acting as a client's legal guardian;
2. Functioning *in loco parentis*;
3. Persons other than a parent who have been authorized by the court or state law to make health care decisions for the client; OR
4. The executor, administrator, or other person that has the right to act on behalf of a deceased client (or that client's estate).

B. Exceptions to the general rule of parental/personal representative control include:

1. When state law does not require consent of a parent/personal representative before a minor can obtain a particular form of treatment, such as HIV testing and mental health services, the minor controls information associated with that treatment;
2. When a parent/personal representative agrees to a confidential relationship between CPH and a minor, the personal representative does not have access to the information associated with that agreement unless the minor permits it;
3. When CPH has a reasonable belief that a child has been, or may be, subject to abuse or neglect, or that providing information to a parent/personal representative could endanger the minor, CPH may choose not to disclose;
4. CPH may withhold information from a parent/personal representative if in the exercise of its professional judgment, CPH has decided that it is not in the best interests of the minor client to treat the parent/personal representative as the client's personal representative.

## **215-RM Disclosure of Protected Health Information Related to Organ and Tissue Donations**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Protected Health Information Related to Organ and Tissue Donations
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>215-RM</b>

### **PURPOSE**

The intent of this section is to instruct on disclosure of protected health information to organ procurement, banking, or transplantation organizations.

### **POLICY**

CPH may disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes, or tissue donated by clients. No additional consent, authorization, or opportunity to agree or object is required.

## **216-RM Consent to Photograph Clients and/or Use of Clients' Statements**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Consent to Photograph Clients and/or Use of Clients' Statements
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>216-RM</b>

### **PURPOSE**

The intent of this section is to instruct on obtaining consent from clients prior to obtaining their photos and/or statements.

### **POLICY**

1. Prior to obtaining pictures for educational, publicity or other purposes, the client's signature is obtained on a Consent for Pictures and Statements form (Attachment 202.1 RM J).
2. Prior to the release of the client's pictures from his/her medical record, an authorization to release information must be obtained from the client.

## **217-RM Verification of Callers on Telephone Requests for Protected Health Information**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Verification of Callers on Telephone Requests for Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>217-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the need for proper identification/verification to ensure that the requestor is entitled to receive the protected health information.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. TELEPHONE INFORMATION RELEASE**

- A. Persons calling are strongly encouraged to put requests in writing. If this is not feasible due to the nature or urgency of need:
  - 1. The caller's name and telephone number is taken.
  - 2. The information is released later on a call-back basis.
- B. For programs that may legally release protected health information via telephone, clients may receive test results:
  - 1. During the designated call-in time; *and*
  - 2. After proper identification is verified.
- C. When such information is released, the following are recorded on a progress note and placed in the client's record:
  - 1. The information released.
  - 2. To whom the release was made.
  - 3. The date and time of the conversation.

## **218-RM Disclosure of Psychotherapy Notes**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Psychotherapy Notes
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>218-RM</b>

### **PURPOSE**

The intent of this section is to instruct on instances when such notes may be released without an authorization from the client.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. PSYCHOTHERAPY NOTES**

Appropriate authorization is necessary to disclose psychotherapy notes for a client except under the following circumstances:

- A. For the practitioner who wrote the notes for treatment of the client;
- B. For students, trainees or practitioners in supervised training programs;
- C. To defend CPH against legal action or other proceedings brought against CPH by the client;
- D. For lawful health oversight activities or as otherwise required by law;
- E. For coroners or medical examiners in cases in which the client is deceased;
- F. When CPH believes, in good faith, that the use or disclosure of the protected health information is needed to prevent or lessen a serious threat to health or safety

## **219-RM Appropriate Authentication and Signatures for Consent to Release Protected Health Information (PHI)**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Appropriate Authentication and Signatures for Consent to Release Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	4/20/2004
<b>REFERENCE NUMBER:</b>	<b>219-RM</b>

### **PURPOSE**

The intent of this section is to instruct on obtaining signatures for the release of protected health information under various circumstances.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. APPROPRIATE AUTHENTICATION AND SIGNATURES**

Signatures for the release of protected health information are obtained as follows in the described circumstances:

- A. If the client is unconscious or incompetent, the signature of the legal guardian or next of kin (spouse, parent, adult child in that order) must be obtained. Relationship is to be clearly documented on the Authorization to Release Information form.
- B. If the client has signed a limited or general Power of Attorney form, the individual given power of attorney may sign for the client and have access unless the client becomes medically incapacitated.
- C. If the client has signed a durable Power of Attorney form for health care, the individual given power of attorney may sign and have access even in the event the client becomes incapacitated. The Power of Attorney form must state authorization and/or copies of the medical record may be given to the individual given power of attorney.
- D. If the client is only able to make an "X" or other marking, an adult must witness the authorization for release of information. If the client is completing the authorization onsite, a CPH employee may witness it. Also, CPH employee must document on the authorization that the client can only sign with an "X" or other marking.
- E. If the client is a minor, the parent, guardian, or legal custodian may sign. Court documentation is required to prove guardianship or legal custody. Married minors are permitted to sign for themselves and their children, as well as minors being treated for drug or alcohol abuse, sexually transmitted diseases or related infectious diseases, or clients receiving WIC Program services.
- F. If the client is deceased, and his/her estate has been established in Probate Court, the client's protected health information may be released when:
  1. The executor/executrix of the client's estate signs a valid authorization; OR
  2. A valid court order is issued for the information.

- G. However, if the deceased client's estate has been opened and the estate's assets have been distributed, and the estate has been closed in Probate Court, the release may occur when the individual requesting the protected health information obtains a court order from Probate Court.
- H. If the client has died intestate (without a will) and indigent (without appreciable assets), usually an estate is not established in Probate Court. In this case, the information may be released when the individual requesting the protected health information obtains a court order from Probate Court.
- I. If the request for protected health information is part of a legal action, in which the deceased client is a plaintiff, a defendant, or neither, a court order from the court in which the lawsuit is filed would suffice for the release of the information.

# **220-RM Processing Written Requests for Protected Health Information**

## **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Processing Written Requests for Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	3/17/2005
<b>REFERENCE NUMBER:</b>	<b>220-RM</b>

## **PURPOSE**

The intent of this section is to instruct on the release of protected health information upon receipt of a written request for copies of protected health information other than public records requests

## **PROCEDURES & STANDARD OPERATING GUIDELINES**

### **I. PROCESSING WRITTEN REQUESTS FOR PROTECTED HEALTH INFORMATION**

- A. Upon receipt of a written request for copies of protected health information, the program designee will mark the date received on the request and verify whether the client was seen by the program
- B. If no record can be found, ask the requestor for additional identifying information. When the information is obtained, route the request to the appropriate program
- C. If there is a record of the client, check the authorization for compliance with the guidelines set forth in the Authorization to Release Information policy and procedure. If the authorization does not contain all of the necessary elements, or there is not a valid authorization form, notify the requestor via the Returned Request for Release of Protected Health Information form and send them a CPH Authorization to Release Information form.

Photocopy **ONLY** the minimum necessary information if the authorization meets the guidelines.

For programs that charge for copies, the maximum charges allowed by law for copying protected health information are listed in the Privacy Notice.

Copies of client records shall be released without charge to:

- A. The client or his/her personal representative for continuity of the client's medical care;
- B. The client or the client's personal representative for the first copy only if the record is necessary to support a claim for Social Security disability benefits and the request is accompanied by documentation that the claim has been filed, as mandated by Sub. HB 331;
- C. A physician or health or social service care providers who are treating the client;
- D. Internal department/program committees for the purpose of quality assurance, client care evaluation, service or program reviews, or management or financial audits;
- E. Governmental agencies as required by law;
- F. Bureau of Workers Compensation;
- G. Lawful court orders;
- H. Law enforcement authorities;
- I. The Industrial Commission;
- J. The Department of Job and Family Services;

---

K. The Attorney General of the State of Ohio.

Attach a copy of the Authorization to Release Information form prior to sending the copies to the requestor.

- A. File the original authorization form in the client's record. Include the following information:
- B. What portions of the record were copied and sent;
- C. The date the copies were sent;
- D. The full name and address of the individual or entity to whom the copies were sent; and
- E. The name of the staff member who prepared and sent the copies.

## **221-RM Disclosure of Protected Health Information to Health System Oversight Entities and Other Governmental Entities**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Protected Health Information to Health System Oversight Entities and Other Governmental Entities
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>221-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the release of protected health information without client authorization to health oversight and governmental agencies.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. DISCLOSURE OF PROTECTED HEALTH INFORMATION POLICY**

CPH may use and disclose protected health information without client authorization to:

- A. A health oversight agency for audits, or for civil, administrative, or criminal actions, inspections, licensure or disciplinary actions;
- B. Appropriate military command authorities of either the United States or foreign countries for activities deemed necessary to assure the proper execution of a military mission;
- C. Federal officials for conducting national security activities as authorized under the National Security Act of 1947;
- D. Federal officials for protection of either the President of the United States or foreign heads of state.

CPH must receive an appropriate, signed authorization from an inmate before disclosing the inmate's protected health information to a correctional institution or a law enforcement official having lawful custody of the inmate.

**NOTE:** An individual is no longer an inmate when released on parole, probation, supervised release or otherwise is no longer in lawful custody.

All requests for protected health information from any of the entities mentioned above must be in writing. These requests will be routed to the program manager or designee of the appropriate program area within 2 workdays of receiving the request.

#### **II. DISCLOSURE OF PROTECTED HEALTH INFORMATION PROCEDURE**

- A. The program manager or designee will:
  - 1. Determine whether the request for information meets any of the criteria listed in the policy above and is therefore valid; OR

- 
2. Contact the requesting party to obtain more information to determine the validity of the request, if necessary.
- B. If the program manager or designee still doubts the request's validity after obtaining additional information from the requestor, he/she will:
1. Fax the request to the city attorney; and
  2. Request a consultation from the city attorney regarding the need for additional authorization from the client or his/her personal representative prior to releasing the information.
- C. If additional authorization is needed, the program manager or designee will inform the requestor of this. Please refer to the policy and procedure regarding Authorization to Release Information.
- D. If the program manager or designee determines that the request is valid, the record will be prepared for review by the requestor.
1. Review the record to ensure that it is complete, the signatures are identifiable and each page of the record contains the client's name and, if applicable, identification number.
  2. Check the record to ensure that only those items specifically requested are included prior to photocopying or submission for on-site review. Information not specifically requested should be omitted.
  3. When photocopying, make a list of the specific documents that have been copied and place it in the original medical record.

In the case of onsite reviews, the program manager or designee will verify the reviewer's name and credentials by comparing the reviewer's driver's license or state identification card to his/her work identification card or badge prior to the reviewer gaining access to the records.

## **222-RM Disclosure of Client Information - Mass Vaccinations**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Disclosure of Client Information- Mass Vaccinations
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>222-RM</b>

### **PURPOSE**

The intent of this section is to establish a policy to safeguard the protected health information of clients immunized by Columbus Public Health (CPH) via mass vaccinations.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. DISCLOSURE OF CLIENT INFORMATION POLICY**

Written authorization from clients or their personal representatives is required before protected health information (PHI) is released, disclosed or made available for review **except** where a specific law, regulation, or approved administrative need requires or permits such access without the client's/personal representative's authorization.

- A. Lists containing the names of multiple clients who received vaccinations may be released without the client's/personal representative's authorization to the following entities (45 CFR, section 164.512):
  1. United States government agencies conducting public health surveillance, investigations or interventions;
  2. Foreign government agencies acting in collaboration with a United States public health authority, provided that the United States public health authority has authorized the release of the PHI;
  3. Entities subject to FDA jurisdiction, such as vaccine manufacturers, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that entity has responsibility. This includes, for example, collecting or reporting adverse events involving food and dietary supplements, product defects or problems, or biological product deviations;
  4. CPH staff members who are responsible for certain administrative, financial, legal and quality improvement activities that are necessary to running the business and to support core functions of treatment and payment. This includes, for example, conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health costs, and case management and care coordination;
  5. Individuals or entities that provide documentation that an alteration or waiver of research participants' authorization for the use and disclosure of PHI has been approved by an Institutional Review Board (IRB) or a Privacy Board. This includes, for example, conducting records research, when researchers are
  6. unable to use de-identified information, and the research could not practicably be conducted if the research participants' authorization was required;
  7. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to investigate complaints regarding HIPAA violations or to otherwise ensure compliance;
  8. Law enforcement, which can, under specified conditions, receive PHI pursuant to a court order, subpoena, or other legal order, to help identify and locate a suspect, fugitive, or missing person. Please see policy #209-RM, Policy for Responding to Subpoenas and Court Orders; and
  9. Judicial and administrative entities under specified circumstances. Please see policy #208-RM, Policy for Responding to Subpoenas and Court Orders.

- 
- B. Lists containing the names of multiple clients who were vaccinated will not be released to the following entities:
1. News media entities or representatives; and
  2. Any other individuals or entities not appearing in the above list.
- C. CPH may release vaccination information regarding a **specific** client without the client's/personal representative's authorization to health care providers who are providing *emergency* treatment to that client and need the information for continuity of care purposes. However, CPH must attempt to obtain authorization as soon as reasonably possible after delivery of treatment. If authorization cannot be obtained, CPH must document in the client's medical record its attempts to obtain authorization and the reason it could not obtain authorization (45CFR, section 164.506(a)).

## 223-RM Release of Protected Health Information to Law Enforcement

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Release of Protected Health Information to Law Enforcement
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>223-RM</b>

### **PURPOSE**

The intent of this section is to establish a policy for the release of protected health information when it is requested by law enforcement officials in the pursuit of their duties.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. DISCLOSURE OF PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT**

CPH may disclose protected health information for law enforcement purposes to a law enforcement official under several sets of circumstances. **EXCEPTION: For cases involving the alcohol and/or drug abuse program, please refer to 42 CFR, Part 2.**

##### **A. *Law Enforcement Officials***

A law enforcement official is an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, and who is empowered to:

1. Investigate or conduct an official inquiry into a potential violation of law; OR
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

##### **B. *Positive Identification Required for Law Enforcement Officials***

1. Individuals claiming to be law enforcement officials must provide positive, photographic identification of their personal identity, as well as their law enforcement identification. Business cards are NOT acceptable for this purpose.
2. All forms of identification presented by law enforcement officials will be photocopied by CPH staff and placed in the medical record(s) of the client(s) whose information is requested by the officials.

##### **C. *Disclosures Required by Law***

CPH may disclose protected health information as required by specific laws, such as those that require the reporting of certain types of wounds or injuries, such as gunshots, child abuse and neglect, etc.

CPH may disclose protected health information in compliance with:

1. A court order or court-ordered warrant;
2. A subpoena or summons issued by a judicial officer;
3. A grand jury subpoena; OR

4. An administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand, or a similar process authorized under law.

The information sought in the circumstances listed above must be:

1. Relevant and material to a legitimate law enforcement inquiry;
2. Specific and limited in scope to the extent possible in view of the purpose for which the information is sought; AND
3. For a purpose for which de-identified information could not reasonably be used.

#### ***D. Disclosures Related to Crime Investigations***

CPH may disclose protected health information for the identification and location of a suspect, a fugitive, a material witness, or a missing person. In such cases, CPH may only disclose the following:

1. Name and address;
2. Date and place of birth;
3. Social security number;
4. ABO blood type and rh factor;
5. Type of injury;
6. Date and time of treatment;
7. Date and time of death, if applicable; AND
8. A description of distinguishing physical characteristics, including weight, height, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos.

The following are **excluded** from the above list:

1. Typing, samples or analysis of body fluids or tissue (unless it is one of the items listed above);
2. DNA or DNA analysis; AND
3. Dental records.

#### ***E. Disclosure of PHI With Client's Authorization***

CPH may disclose protected health information in response to a law enforcement official's request for such information about a client who is, or is suspected to be, a victim of a crime, if the client authorizes the disclosure.

#### ***F. Disclosure of PHI Without Client's Authorization***

CPH may also disclose even without the client's authorization if the client is incapacitated or under other emergency circumstances, as long as:

1. Law enforcement officials represent that such information is needed to determine whether a violation of law by a person other than the client has occurred, and such information is not intended to be used against the client;
2. Law enforcement officials represent that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the client is able to agree to the disclosure; and

3. The disclosure is in the best interest of the client as determined by CPH in the exercise of its professional judgment.

***G. Death of a Client***

CPH may disclose protected health information about a client who has died to law enforcement officials for the purpose of alerting them to the suspicion that the death may have resulted from criminal conduct.

***H. Criminal Activity at CPH***

CPH may disclose protected health information to a law enforcement official if CPH believes in good faith that it constitutes evidence of criminal conduct that occurred on CPH's premises.

***I. Reporting Crime While Responding to an Off-site Emergency***

CPH may disclose protected health information if CPH is rendering emergency health care in response to a medical emergency off CPH's premises, and CPH believes that such disclosure is necessary to alert law enforcement officials to the:

1. Commission and nature of the crime;
2. Location of the crime or of the victim(s) of the crime; AND
3. Identity, description, and location of the perpetrator of the crime.

## **225-RM Public Health PHI Disclosures**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Public Health PHI Disclosures
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>225-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the disclosure of protected health information to public health entities or other entities entitled by law to collect or receive it for public health purposes.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. DISCLOSURE OF PROTECTED HEALTH INFORMATION**

CPH, as a public health authority, may disclose protected health information without the authorization of the client to public health authorities or other agencies that are authorized by law to collect or receive such information. The minimum necessary standard applies to all disclosures for public health purposes. **It is recommended that this policy be used for guidance. The final authority rests with the Health Commissioner and the City Attorney.**

**CPH may disclose protected health information for public health purposes under the following circumstances:**

- A. To the general public for programs having open public records, such as birth and death certificates, as long as the amount of information released is only the minimum necessary or as otherwise required by law;
- B. To a public health authority that is authorized by law to collect or receive such information for the purpose of:
  1. Preventing or controlling disease, injury or disability;
  2. Reporting vital events, such as birth or death;
  3. Conducting public health surveillance, investigations or interventions;
  4. Reporting child abuse or neglect;
  5. Oversight activities authorized by law, including:
    - i. Audits;
    - ii. Civil, administrative, or criminal investigations, inspections, licensure or disciplinary actions;
    - iii. Civil, administrative or criminal proceedings or actions; or
    - iv. Other activities necessary for the appropriate oversight of:
      - a. The health care system;
      - b. Government benefits programs for which health information is relevant to beneficiary eligibility;
      - c. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; OR
      - d. Entities subject to civil rights laws for which health information is necessary for determining compliance;
      - e. To an official of a foreign government agency engaged in a collaborative effort if directed to do so by a public health authority;
      - f. To the Food and Drug Administration for purposes related to the quality, safety or effectiveness of FDA-regulated products or activities, including:

1. Collecting or reporting adverse events or similar activities regarding food or dietary supplements, product defects or problems, including problems with the use or labeling of a product, or biological product deviations;
2. Tracking FDA-regulated products;
3. Enabling product recalls, repairs, or replacement, or for look back, including locating and notifying clients who have received products that have been withdrawn, recalled, or are the subject of look back; AND
4. Conducting post-marketing surveillance.
  - aa. To any other public health authority that is authorized to receive or collect reports on adverse events;
  - bb. To notify an individual who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition (OAC 3701-36-06);
  - cc. To notify an employer about a client who may be at risk of spreading a disease or a condition so that the employer may comply with federal or state law to record such illness or injury or carry out responsibilities for workplace medical surveillance (OAC 3701-36-06). Efforts must be made to avoid disclosing the client's identity, although circumstances may arise that would necessitate the release of the client's name (ORC 3701.16).
  - dd. To notify a school administrator, church administrator or any individual responsible for a public gathering about a client who may be at risk for spreading a disease or a condition. Efforts must be made to avoid disclosing the client's identity, although circumstances may arise that would necessitate the release of the client's name (ORC 3707.16).

**CPH may also disclose de-identified data and limited data sets but must make sure that specific guidelines are followed:**

**A. *De-identified data:*** identified data which is aggregate statistical data or data stripped of identifying information may be shared without individual privacy protection. De-identification of data can be achieved by either of the methods described below:

1. Statistical de-identification which involves a *qualified* statistician ensuring that accepted analytic techniques cannot be used alone or in combination with other available information to identify the subject of the information.
2. The safe-harbor method which involves de-identifying information by removing 18 identifiers and ensuring that the remaining information cannot be used alone or in combination to identify the subject. The 18 identifiers are as follows:
  - i. Names
  - ii. Geographic sub-divisions smaller than a state, including county, city, street address, precinct, zip code and equivalent geocodes - ***these include sub-divisions that have less than 20, 000 people;*** however, the first 3 digits are excluded from the PHI list if the geographic unit formed by combining zipcodes with the first 3 digits contains more than 20,000 people.
  - iii. All elements of dates (except year) directly related to an individual, all ages >89;
  - iv. Telephone numbers
  - v. Fax numbers
  - vi. Electronic mail addresses
  - vii. Social security numbers
  - viii. Medical record numbers
  - ix. Health plan beneficiary numbers
  - x. Account numbers

- xi. Certificate and license numbers
- xii. Vehicle identifiers and serial numbers, including license numbers
- xiii. Medical device identifiers and serial numbers
- xiv. Internet universal resource locators (urls)
- xv. Internet protocol addresses
- xvi. Biometric identifiers including fingerprints and voice prints
- xvii. Full-face photographic images and any comparable images
- xviii. Any other identifier that CPH may have assigned

**B. Limited Data Sets:**

1. CPH may include the following PHI without authorization in a limited data set for public health, research or health care operations:
  - i. Town, city, state or zip code
  - ii. Elements of dates related to a person such as years, birth dates, admission dates, discharge dates and dates of death.
2. However, to disclose this limited data set, CPH must enter into a data-use agreement with the recipient organization or individual. This agreement must ensure that the recipient will:
  - i. Not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
  - ii. Use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the data-use agreement;
  - iii. Report to CPH any use or disclosure of the information that is in violation of the agreement;
  - iv. Ensure that any agents to whom it provides the limited data set also agree to the same restrictions and conditions that apply to the limited data set; and
  - v. Not attempt to re-identify the information or contact the individual.

- C. Surveillance:** CPH may disclose PHI collected directly from persons by a person, agency or institution that is not a covered entity, including individually identifiable information. All such disclosures must, however, be authorized by the designated Privacy Officer.

## **226-RM Release of Public Health Information to the Media**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Release of Public Health Information to the Media
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>226-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the processing of public health information requests from media outlets.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. REQUESTS FOR PUBLIC HEALTH INFORMATION**

When requests for public health information are received from media outlets, such as television and radio stations, newspapers, and news wire services:

- A. The requests will be forwarded to Columbus Public Health's Health Communications Director or, in his/her absence, the Health Commissioner; and
- B. The Health Communications Director or, in his/her absence, the Health Commissioner, will communicate to the media outlet all final decisions regarding what information may be released, based upon discussions with:
  1. The City Attorney's office;
  2. Columbus Public Health's Privacy Officer; and
  3. Other individuals, as needed.
  4. CPH employees, volunteers, students and interns who receive media requests for potential public information will:
  5. Obtain the requestor's contact information;
  6. Assure the requestor of a response from the Health Communication Director or, in his/her absence, the Health Commissioner; and
  7. Forward the requestor's needs and contact information to the Health Communications Director or in his/her absence, the Health Commissioner within 1 workday.
- C. The Health Communications Director or, in his/her absence, the Health Commissioner will review the request for potential public health information, and will consult with the City Attorney's office and Columbus Public Health's Privacy Officer, as appropriate. The Health Communications Director or, in his/her absence, the Health Commissioner will then make a determination as to whether it involves information that is:
  1. Mandated by law to be available to the public and may therefore be released to the requestor; *or*
  2. Not mandated by law to be made available to the public and/or is classified as *protected health information* under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- 
- D. If the information is public health information as defined by HIPAA, the Health Communications Director or, in his/her absence, the Health Commissioner, will not release the information to the media.

# **304-RM Security of Protected Health Information Stored Electronically**

## **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Security of Protected Health Information Stored Electronically
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>304-RM</b>

## **PURPOSE**

The intent of this document is to instruct on the protection of portable computing devices and removable storage components containing protected health information from unauthorized access.

In addition, the individual or agency using the above mentioned items must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

- I. **Identity Information:** Data elements regarding an individual that are not connected to that individual's health information but could be used to identify the individual and could potentially render the individual vulnerable to identify theft if misused. See Identifiers in this policy for a list of those data elements.
- II. **Portable Computing Device:** Computer or device designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices, such as flash drives, CD-ROMs, diskettes or other such media.
- III. **Protected Health Information:** Individually identifiable information that is maintained or transmitted that:
  - A. Is created or received by an entity covered under HIPAA, such as CPH;
  - B. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual;
  - C. Identifies the individual with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and
  - D. Includes the data elements listed under Identifiers in this policy.

## **PROCEDURES & STANDARD OPERATING GUIDELINES**

### **I. PROTECTION OF ELECTRONICALLY STORED INFORMATION**

Please refer to Executive Order 2007-3 for more information.

- A. Users will protect portable computing devices and removable storage components such as diskettes, CD's, DVD's and flash memory cards from unauthorized access. Physical security measures will include at a minimum:
- B. Devices shall not be left unattended without employing adequate safeguards such as cable locks, restricted access environments or lockable cabinets.

- C. When possible, devices shall remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device, computer media and removable components.
- D. Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.
- E. An inventory will be developed and given to program managers to be maintained on an ongoing basis for each CPH-owned portable device authorized for work use with CPH's systems. The inventory will include the:
  - 1. Device make;
  - 2. Device model number;
  - 3. Device serial number;
  - 4. Date the device was introduced into service;
  - 5. Party responsible for the device; and
  - 6. A periodic inventory of the protected health information and/or identity information stored in the device to be compiled each day the device is in use.
  - 7. Prior to removal of portable devices from the building, backup copies of data must be created and stored in a secure area.
  - 8. Authorization must be obtained prior to the purchase of portable devices. The approval form is located on the intranet at:  
<http://intranet/Health2/Lists/Purchase%20Request/NewForm.aspx?Source=http%3A%2F%2Fintranet%2FHealth2%2FLists%2FPurchase%2520Request%2Foverview%2Easpx>
- F. Before removal from the premises, protected health information stored on either portable media, such as flash drives, floppy disks, etc., or in electronic or hardcopy form must be pre-approved via a manager's signature.
- G. Before removal of protected health information from the premises, data inventories detailing the contents of any item containing protected health information, such as those items listed in item E above, must be compiled.
- H. Methods for securing protected health information and/or identity information stored on portable devices or media may include but are not limited to:
  - 1. Personal **firewalls**;
  - 2. BIOS passwords;
  - 3. Data/application encryption;
  - 4. **Screen locking**;
  - 5. **Screen timeout**; and/or
  - 6. Passwords
  - 7. Personally identifiable information and/or protected health information will NOT be included in e-mails unless the user has been given access to email encryption software.
- I. CPH-owned portable computing devices must be:
  - 1. Promptly returned to the employee's supervisor when the employee terminates from CPH or when his/her assignment no longer requires the use of the device; and
  - 2. Program managers will update the inventory list promptly upon such changes.
- J. CPH will ensure that portable computing device security is addressed in its employees' HIPAA training program.



## **306-RM HIPAA Quality Assurance Monitor**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	HIPAA Quality Assurance Monitor
<b>ORIGINAL DATE ADOPTED:</b>	12/27/2010
<b>REFERENCE NUMBER:</b>	<b>306-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the monitoring of programs for HIPAA compliance.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. HIPAA COMPLIANCE MONITORING**

For quality improvement purposes, all Columbus Public Health programs will be monitored for compliance with HIPAA on a periodic basis. The monitoring process will focus on prevention of access to protected health information by inappropriate individuals. Monitors are to be conducted at least once a year during the third quarter of the calendar year.

Division leadership will be made aware of the results of the monitoring process. Programs found to be deficient will be expected to develop methods, order necessary equipment, etc., to correct the situation in a timely manner.

##### ***A. Each program manager/designee will:***

1. Complete the HIPAA Quality Assurance Monitor Form for the program site for which he/she is directly responsible;
2. Complete the Program Manager's/Designee's Response to Findings and Plan of Corrective Action form if deficiencies are found; and
3. Forward the original of both documents to the HIPAA Steering Committee by the 10<sup>th</sup> working day of the following month.

##### ***B. The HIPAA Steering Committee will:***

1. Forward a legible copy of both documents to the appropriate Division Leader if a program is found to have deficiencies;
2. File both documents in a locked HIPAA Steering Committee file cabinet for safekeeping.

##### ***C. If any deficiencies are identified, the program manager/designee will:***

1. Alert the appropriate Division Leader within 2 workdays;
2. Complete the Program Manager's / Designee's Response to Findings and Plan of Corrective Action within 5 workdays; and
3. Perform a second audit within 30 days of completion of the corrective action plan described above to assess progress in implementing necessary changes.

- 
4. The second audit will be forwarded to the HIPAA Steering Committee by the 10<sup>th</sup> working day of the month following the date of the second audit.

## **307-RM Notification in the Case of Breach of Unsecured Protected Health Information**

### **POLICY AND PROCEDURE**

<b>SUBJECT/TITLE:</b>	Notification in the Case of Breach of Unsecured Protected Health Information
<b>ORIGINAL DATE ADOPTED:</b>	01/15/2011
<b>REFERENCE NUMBER:</b>	<b>307-RM</b>

### **PURPOSE**

The intent of this section is to instruct on the notification of clients whose protected health information (PHI) has been disclosed in a manner inconsistent with Federal law.

### **GLOSSARY OF TERMS**

The following definitions are relevant to this document.

#### **Breach also excludes:**

- A. Any unintentional acquisition, access or use of PHI by a CPH employee or a person acting under the authority of a business associate of CPH if the acquisition, access or use was made in good faith and within the scope of authority without resulting in further use or disclosure.
  - B. Any inadvertent disclosure by a person who is authorized to access the PHI at CPH or one of its business associates to another person authorized to access the PHI at CPH or one of its business associates, as long as the information disclosed is not used or disclosed further.
  - C. A disclosure of PHI where CPH or one of its business associates believes in good faith that the person to whom the PHI was disclosed would not be able to retain it.
- I. **Law enforcement official:** An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
- A. Investigate or conduct an official inquiry into a potential violation of law; or
  - B. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- II. **Unsecured PHI:** PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS) in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS website.

### **PROCEDURES & STANDARD OPERATING GUIDELINES**

#### **I. BREACH**

A breach is considered as having been discovered:

- 1. On the first day on which the breach becomes known to CPH; or

2. Would have been known to any person employed by CPH other than the individual who committed the breach if that person was exercising reasonable diligence.

## **II. CPH's HIPAA Steering Committee (HSC)**

- A. Following the discovery of a breach of unsecured PHI, CPH's HSC will:
  1. Notify each individual whose unsecured PHI has been or is reasonably believed by CPH to have been accessed, acquired, used, or disclosed as a result of such breach;
  2. Coordinate with CPH's Communications Director to develop all media and internet postings and notices;  
AND
  3. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his/her unsecured PHI is included in the breach.
- B. If the HSC feels a breach situation requires urgent notification because of imminent misuse of unsecured PHI, the HSC may provide information to individuals by telephone or other means, as appropriate, in addition to the notice described in Section B above.
- C. If the breach involves **more than 500 residents** of the State of Ohio and/or the Columbus metropolitan area, prominent media outlets serving the State and/or metropolitan Columbus will be notified by the HSC. This notification must occur no more than 60 calendar days following the discovery of the breach.
- D. For breaches involving **500 or more individuals**, the HSC will provide notification to the Secretary of Health and Human Services (HHS) in the manner specified on the HHS website.
- E. For breaches involving **less than 500 individuals**, the HSC will maintain a log or other documentation of these breaches. The HSC will provide the notification of such breaches to the Secretary of HHS no later than 60 days after the end of each calendar year for breaches that occurred during the preceding calendar year in the manner specified on the HHS website.

## **III. BUSINESS ASSOCIATE**

- A. Any business associate of CPH that becomes aware of a breach of unsecured PHI must notify CPH's Privacy Officer or designee of the breach without unreasonable delay and no later than 60 calendar days after the breach's discovery.
- B. The business associate must consider the breach as discovered on the first day on which the business associate becomes aware of the breach, or by exercising due diligence, would have become aware of the breach via any person, other than the person who committed the breach, who is an employee of the business associate, or an officer or other agent of the business associate.
- C. The notification that must be made by the business associate to the Privacy Officer or designee must include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
- D. The business associate will provide the Privacy Officer or designee with any other available information that CPH is required to include in the notification of the individual as described above with updates in information thereafter as information becomes available.

- E. If a law enforcement official states to the Privacy Officer or designee or to any of CPH's business associates that a notification or posting as described above would impede a criminal investigation or cause damage to national security, the Privacy Officer or designee and/or any of CPH's business associates will:
  - 1. Delay the notification or posting if law enforcement's statement is in writing and specifies the required time period for the delay; or
  - 2. Delay the notification or posting for no more than 30 days from the date of law enforcement's statement if law enforcement makes the statement orally and the Privacy Officer or designee or any of CPH's business associates documents the statement, including the identity of the law enforcement official making the statement. There would be an exception to the 30-day time period if a written statement described in Part (a) above was provided by the law enforcement official during that 30-day time period.
- F. If there is a use or disclosure of unsecured PHI, the HSC or any of CPH's business associates must demonstrate by maintenance of sufficient documentation that all notifications were made or that the use or disclosure of the PHI did not constitute a breach.

#### **IV. OTHER**

- A. The HSC must train its workforce on this policy and procedure as necessary and appropriate for its workers to carry out their functions. Workers will be informed that failure to adhere to the policies and procedures may result in disciplinary action.
- B. If individuals wish to complain about CPH's policies and procedures with regard to breaches of unsecured PHI or complain about CPH's lack of compliance with such policies and procedures, they will be directed by CPH staff to contact the Privacy Officer or designee.
- C. CPH may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his/her rights as described above.
- D. CPH may not require individuals to waive their rights as a condition of treatment or payment.

#### **CITATIONS**

Refer to 42 Code of Federal Regulations (CFR), Part 2. (**204-RM**)

#### **CONTRIBUTORS**

The following staff contributed to the authorship of this document:

- 1. Shelly Mitchell, RHIA, Health Information Manager
- 2. Sandra Taylor, RHIA, Franklin County Registrar

#### **APPENDICES**

N/A

## FORMS

### **HIPAA FORMS**

- 201.1 RM A: Confidentiality Agreement
- 202.1 RM A: Authorization to Release Information (English)
- 202.1 RM B: Authorization to Release Information (Spanish)
- 202.1 RM C: Authorization to Release Information (Somali)
- 202.1 RM D: Authorization to Release Information to Alcohol and Drug Abuse Program
- 202.1 RM E: Authorization to Release Information from Alcohol and Drug Abuse Program
- 202.1 RM I: Authorization to Release Information to ADAMH Board from Alcohol and Drug Abuse Program
- 202.1 RM J: Consent for Pictures and Statements
- 202.1 RM AF: Authorization to Release Information for Occupational Health
- 202.1 RM AG: Authorization to Release Blood Testing Information for Minors
- 202. 1 RM AI: Authorization to Release Information to Ohio Childrens Trust Fund
- 202.1 RM AQ: Authorization to Release Immunizations Information for Minors and Dependent Adults
- 202.1 RM HA: Family Ties Authorization to Release Information from CPH to FCCS
- 202.1 RM HB: Family Ties Authorization to Release Information from One Agency to Another
- 202.1 RM HC: Family Ties Authorization to Release Information from CPH to Ohio Childrens Trust Fund OCTF
- 202.2 RM A: Accounting for Disclosures Log (Adults)
- 202.2 RM B: Account for Disclosures Log (Children)
- 202.4 RM A: Notice of Privacy Practices (English)
- 202.4 RM B: Acknowledgement of Receipt of Privacy Notice (English)
- 202.4 RM C: Notice of Privacy Practices (Spanish)
- 202.4 RM D: Acknowledgement of Receipt of Privacy Notice (Spanish)
- 202.4 RM E: Notice of Privacy Practices (Somali)
- 202.4 RM F: Acknowledgement of Receipt of Privacy Notice (Somali)
- 210.0 RM A: Fax Cover Sheet
- 211.0 RM A: Business Associate Privacy Agreement
- 212.0 RM A: HIPAA Customer Complaint Form
- 306.0 RM A: HIPAA Monitoring

## INDEX:

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION (202.2-RM)	16
APPROPRIATE AUTHENTICATION AND SIGNATURES FOR CONSENT TO RELEASE PROTECTED HEALTH INFORMATION (219-RM)	42
AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION (PHI) (202.1-RM)	14
BUSINESS ASSOCIATE PRIVACY AGREEMENTS (211-RM)	32
CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION VIA FACSIMILE (FAX) AND ELECTRONIC MAIL (EMAIL) (210-RM)	30
CONFIDENTIALITY POLICY (201.1-RM)	13
CONSENT TO PHOTOGRAPH CLIENTS AND/OR USE OF CLIENTS' STATEMENTS (216-RM)	39
DISCLOSURE OF CLIENT INFORMATION- DRUG AND ALCOHOL ABUSE PROGRAMS (204-RM)	22
DISCLOSURE OF CLIENT INFORMATION- HIV TESTING OR TREATMENT (203-RM)	20
DISCLOSURE OF CLIENT INFORMATION - MASS VACCINATIONS (222-RM)	48
DISCLOSURE OF PROTECTED HEALTH INFORMATION RELATED TO ORGAN AND TISSUE DONATIONS (215-RM)	39
DISCLOSURE OF PROTECTED HEALTH INFORMATION TO HEALTH SYSTEM OVERSIGHT ENTITIES AND OTHER	
DISCLOSURE OF PSYCHOTHERAPY NOTES (218-RM)	41
GOVERNMENTAL ENTITIES (221-RM)	46
HIPAA CLIENT COMPLAINT PROCESS (212-RM)	33
HIPAA FORMS	66
HIPAA POLICY	4
HIPAA QUALITY ASSURANCE MONITOR (306-RM)	61
INITIATION AND MAINTENANCE OF CLIENT HEALTH RECORDS (101-RM)	9
MINIMUM NECESSARY USE OF PROTECTED HEALTH INFORMATION(202.3-RM)	18
NOTICE OF PRIVACY PRACTICE(202.4-RM)	19
NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (307-RM)	63
PERSONAL REPRESENTATIVES' ROLE IN THE RELEASE OF PROTECTED HEALTH INFORMATION (214-RM)	38
PROCESSING WRITTEN REQUESTS FOR PROTECTED HEALTH INFORMATION (220-RM)	44
PUBLIC HEALTH PHI DISCLOSURES (225-RM)	53
RELEASE OF PROTECTED HEALTH INFORMATION OF CLIENTS EXPERIENCING ABUSE, NEGLECT AND/OR DOMESTIC	
RELEASE OF PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT (223-RM)	50
RELEASE OF PUBLIC HEALTH INFORMATION TO THE MEDIA (226-RM)	56
RESPONDING TO A SUBPOENA OR COURT ORDER (209-RM)	25
SAFEGUARDING PROTECTED HEALTH INFORMATION (102-RM)	11
SECURITY OF PROTECTED HEALTH INFORMATION STORED ELECTRONICALLY (304-RM)	58
VERIFICATION OF CALLERS ON TELEPHONE REQUESTS FOR PROTECTED HEALTH INFORMATION (217-RM)	40
VIOLENCE (213-RM)	35